Cyber Security

For Staff at:

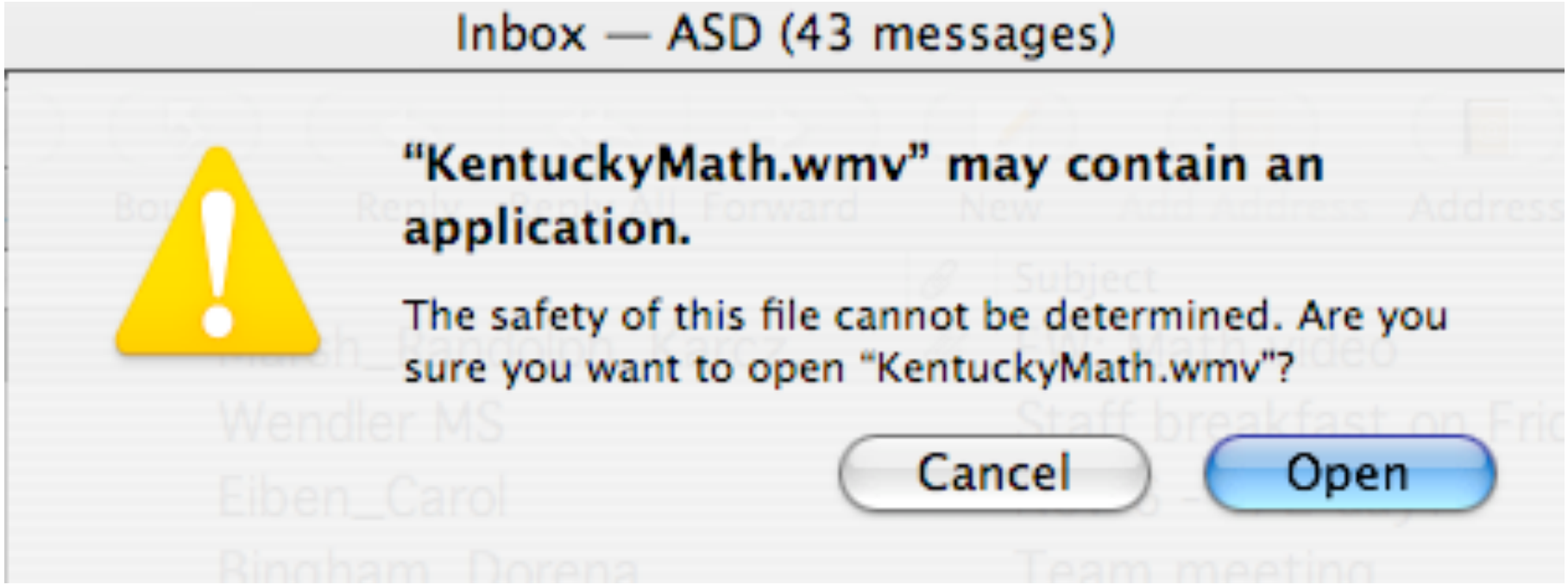
Wendler Middle School

How would you like it if someone came into your class and messed up your stuff????

That’s exactly what can happen to your computer when you aren’t careful!

Something called "malicious code" can get into your computer and mess things up without you even knowing it.

Viruses, worms and Trojan Horses are all types of "malicious code" that can enter your computer and harm or even destroy your files.

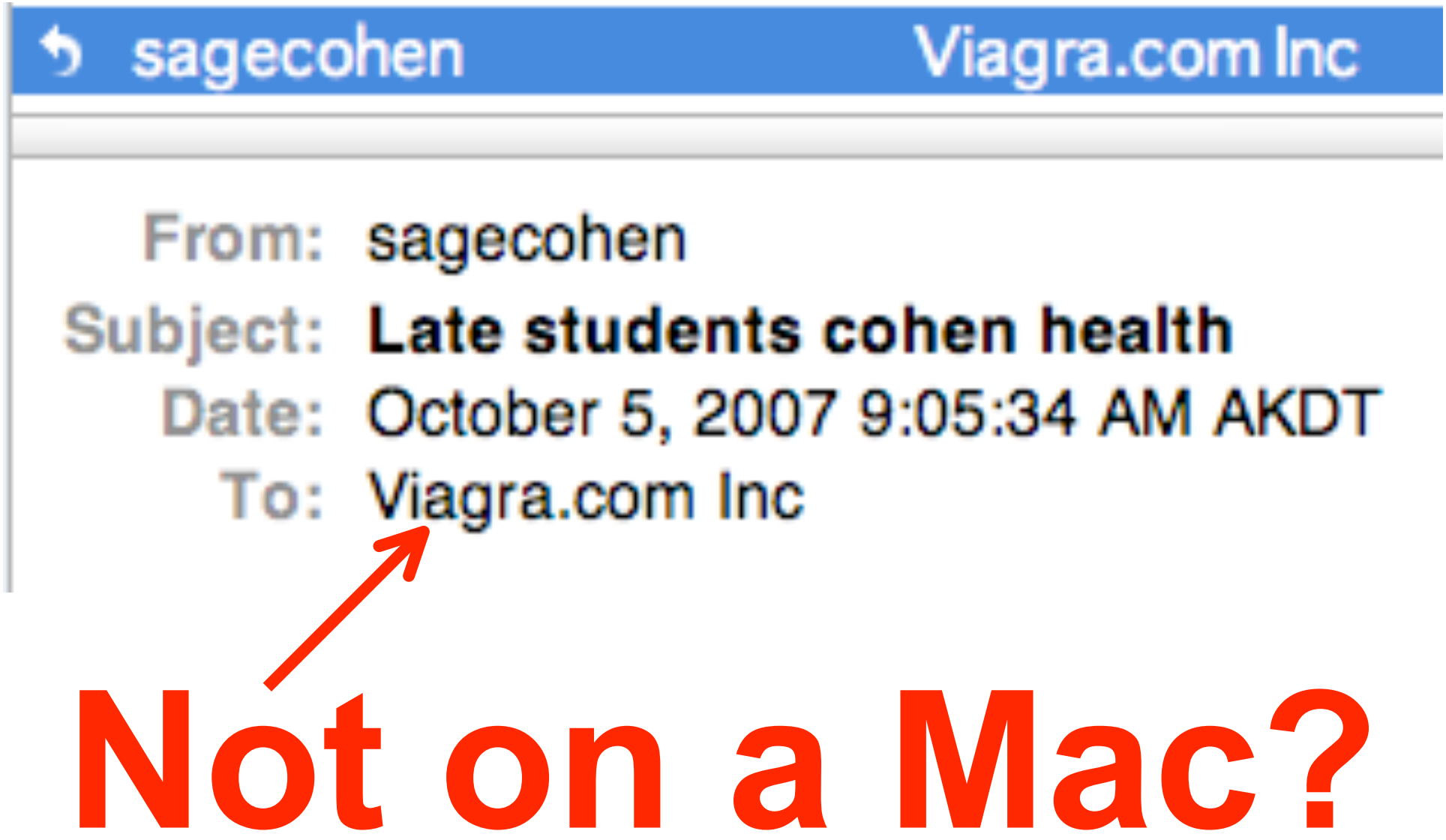

Inbox — ASD (43 messages)
"KentuckyMath.wmv" may contain an application.
The safety of this file cannot be determined. Are you sure you want to open "KentuckyMath.wmv"?
Cancel
Open

114,000 viruses? Not on a Mac.

By the end of 2005, there were 114,000 known viruses for PCs. In March 2006 alone, 850 new threats were detected against Windows. Zero for Mac.

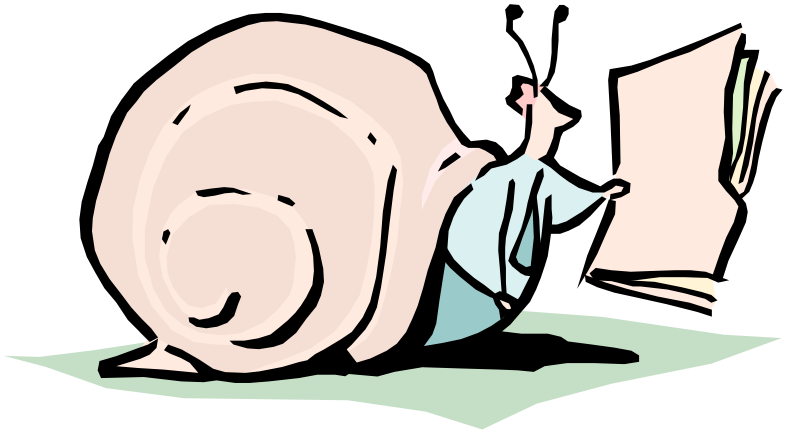
Even Apple says, "no computer connected to the Internet will ever be 100% immune from attack…"

http://www.apple.com/getamac/viruses.html


sagecohen
Viagra.com Inc
From: sagecohen
Subject: Late students cohen health
Date: October 5, 2007 9:05:34 AM AKDT
To: Viagra.com Inc
Not on a Mac?

VIRUS

A ***computer virus*** attaches itself to a program or file so it can spread from one computer to another, leaving infections as it travels.

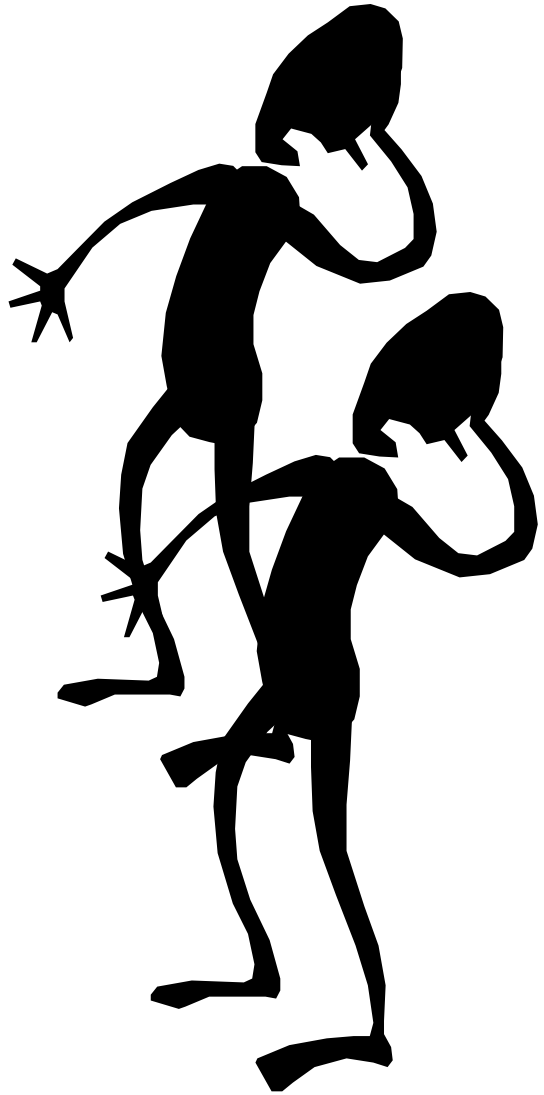


WORMS

Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided, through the network.

TROJAN HORSE

A ***Trojan Horse***, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source.



One way your computer gets infected is through Internet-related activities:

E-mail

I-Ming

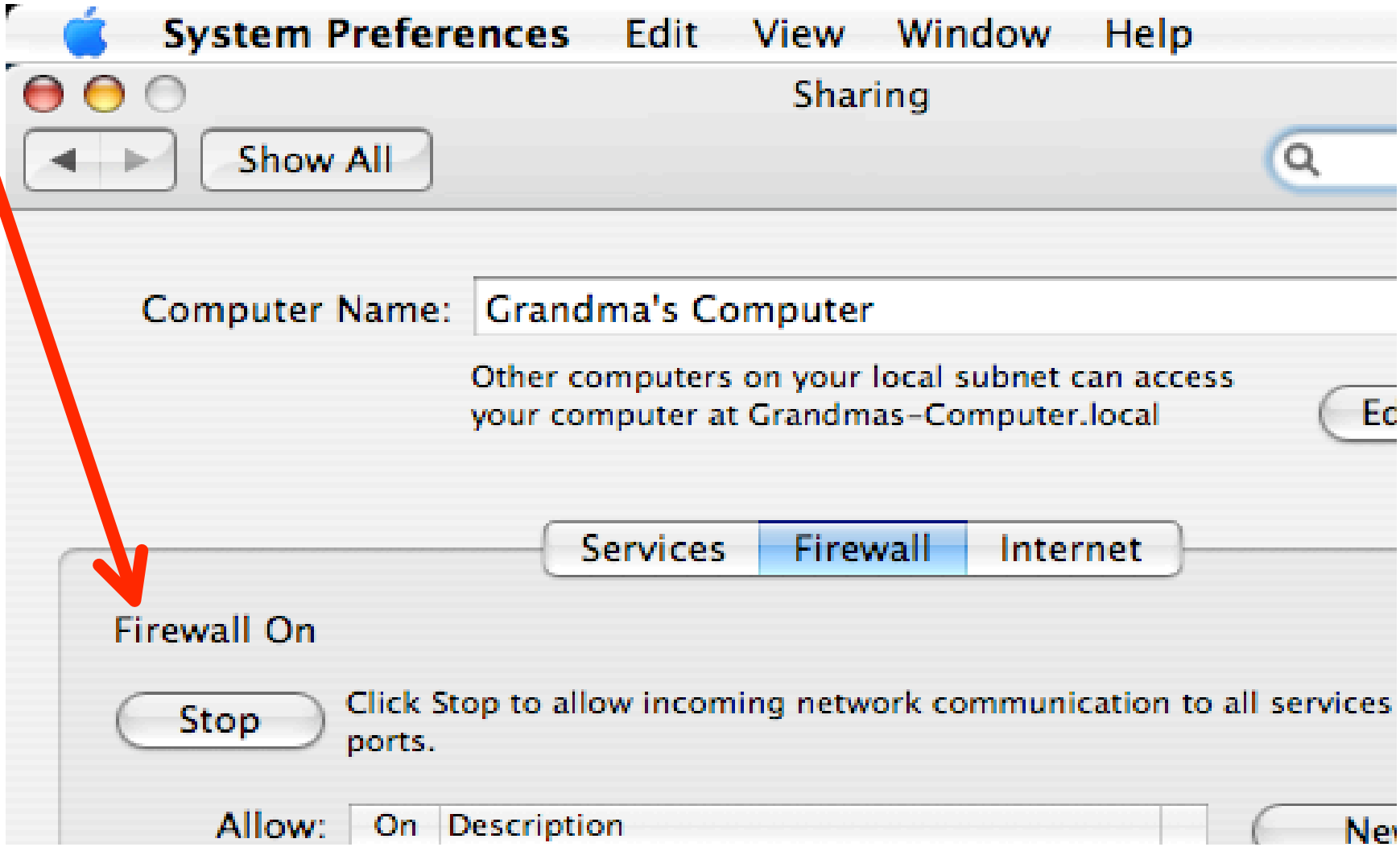
File-sharing

Downloading files

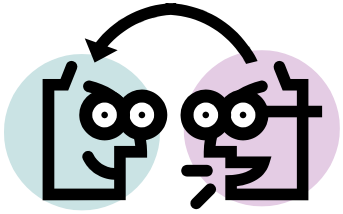
•Don’t open **e-mail attachments** from people you don’t know, or from someone you know, unless you are expecting it and you are sure it is safe.

•Use **anti-virus** software and install a **firewall** on your home computer.

Your Mac has a firewall that you can turn on in your System Preferences, under "Sharing".



Use passwords that are hard to guess by using a combination of letters and numbers.



Don’t share your passwords with anyone.

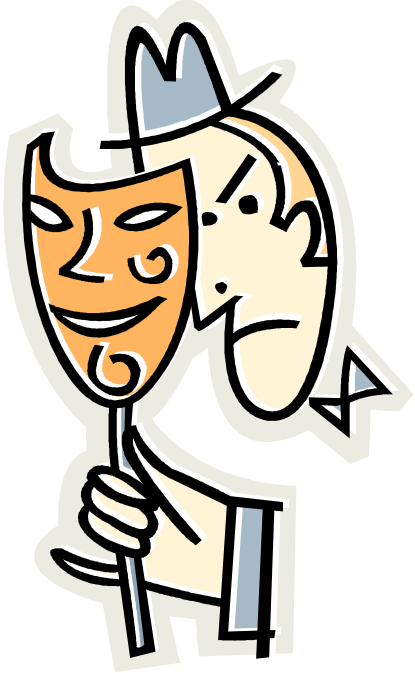
Don’t respond to spam or ‘phish’ email. Your response can lead to more trouble. (Phishing is when someone pretends to be a company such as Amazon or a bank and asks for information.)

- **Disconnect your computer from the Internet when it is not in use.**
- **Don't use file sharing or download software without being confident of its source.**

Use caution before you fall into a hole and can't get out!

Another security problem with the Internet is:

Identity theft!



The best way to prevent identify theft is:

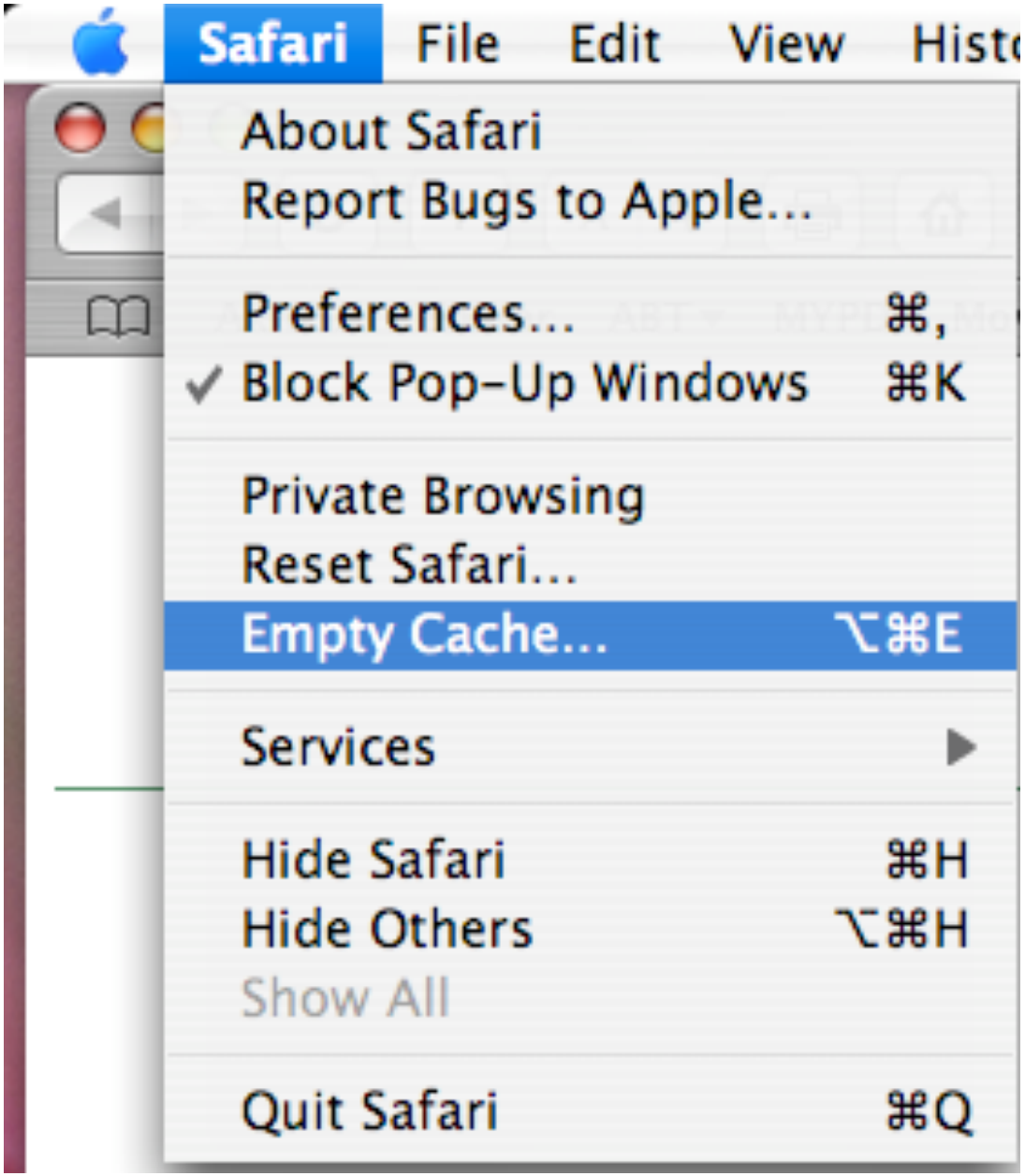
Don't ever give out private information on the Internet.

Some examples of private information are:

Your social security number, your phone number, your full name, or your credit card number.

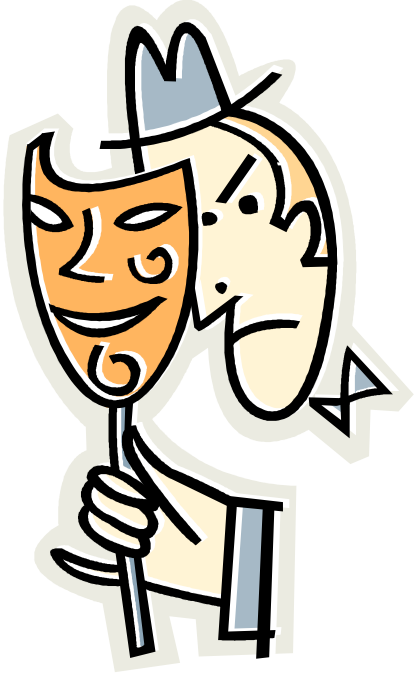
However, if you do business on the Internet, be sure to use an organization you can trust.

Empty the browser **Cache** to prevent others from looking at your page after you walk away.



Another security problem with the Internet is:

Spyware!



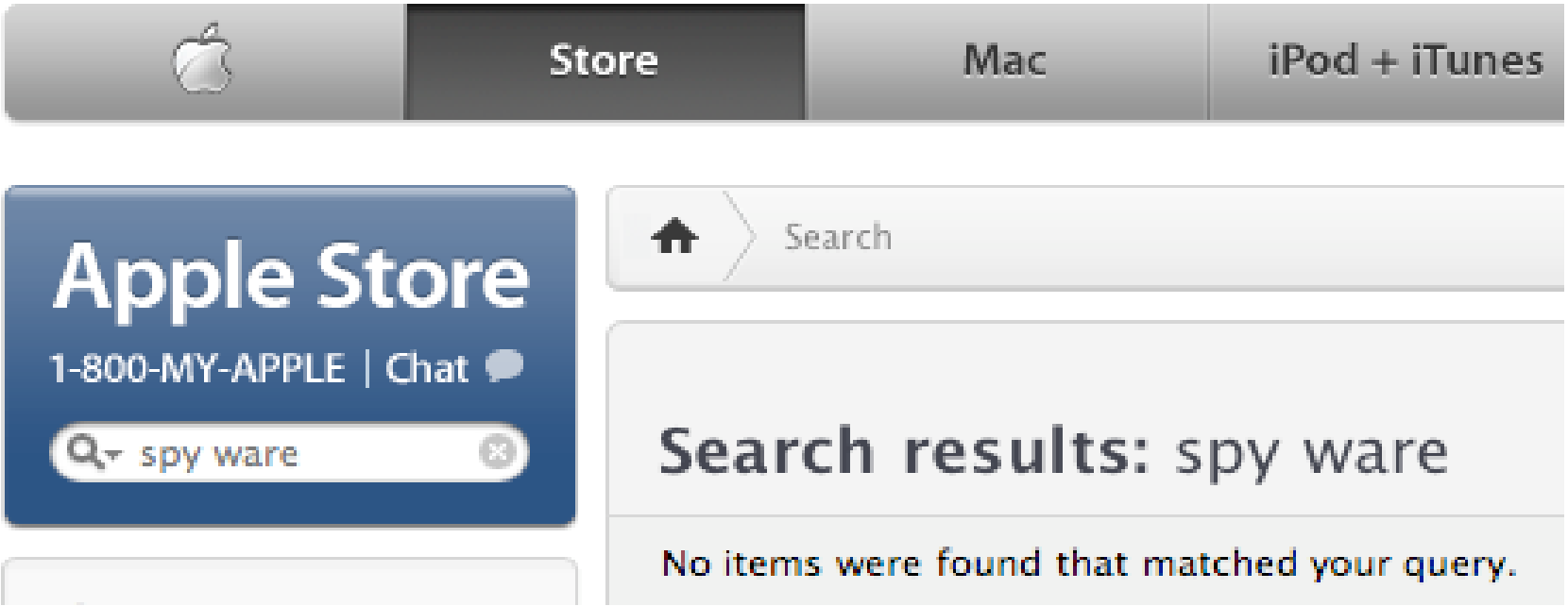
SPYWARE

Spyware is any technology that aids in gathering information about a person or organization without their knowledge.

On the Internet (where it is sometimes called a spybot or tracking software), spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties.

SPYWARE

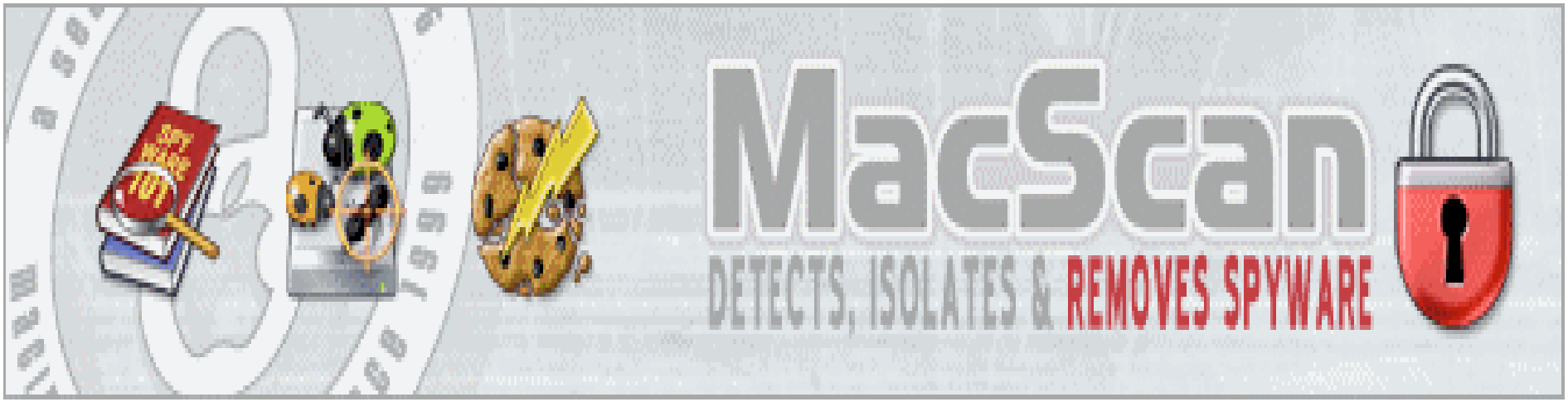
I Googled Apple about Spyware, but got no response. It is a safe bet that they use spyware to gather marketing information. How else could they know which software updates to send you?



SPYWARE

I Googled spyware for a Mac, but personally I do not trust the companies to provide software that is spyware,virus, worm, or trojan free.

I do trust my firewall, however…



Your Mac has a firewall that you can turn on

in your System Preferences, under "Sharing".

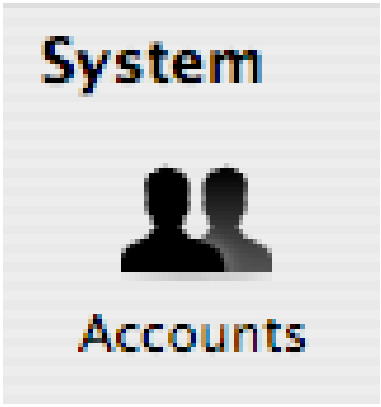
SPYING

Being on a network at school presents another type of spying that can happen.

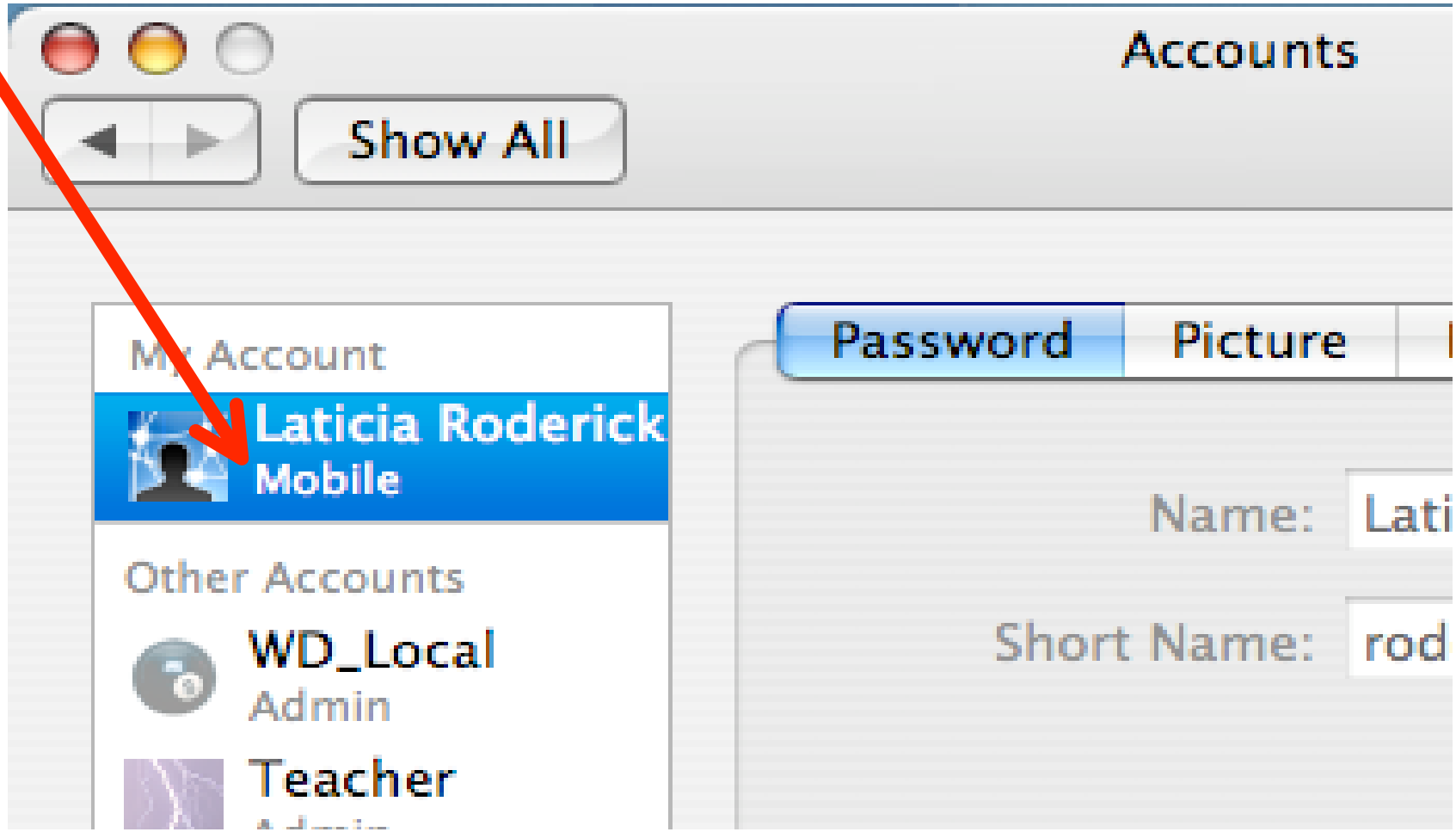
Students (and staff) may have the ability to look in your files, or possibly even at your computer screen when you are writing a confidential email.

Know where your files are… 1) on the **hard drive** of your computer, 2) on the **server** (on the network), or 3) both at the same time (**mobile** account).

SPYING

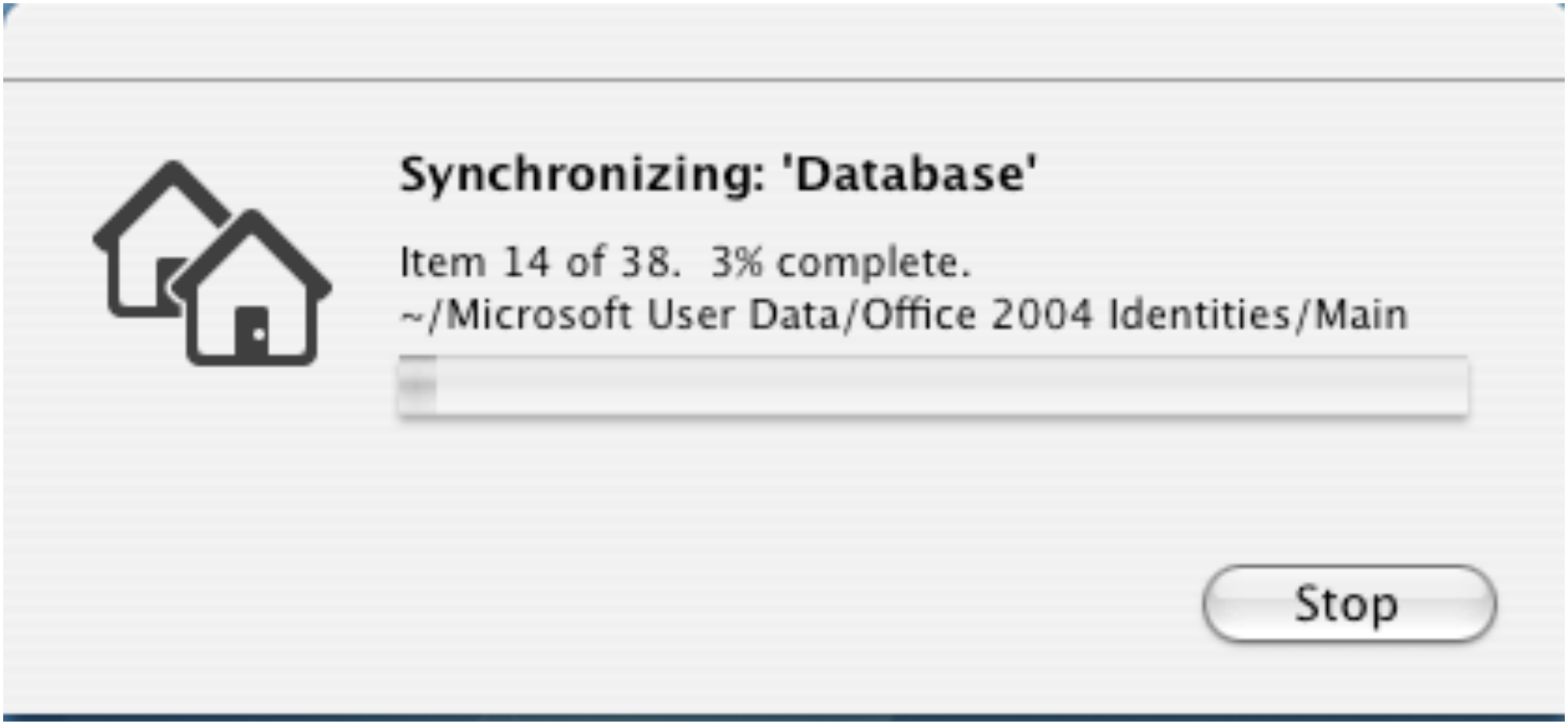


You can look in System Preferences, under **Accounts** to see if you have a **mobile** account.



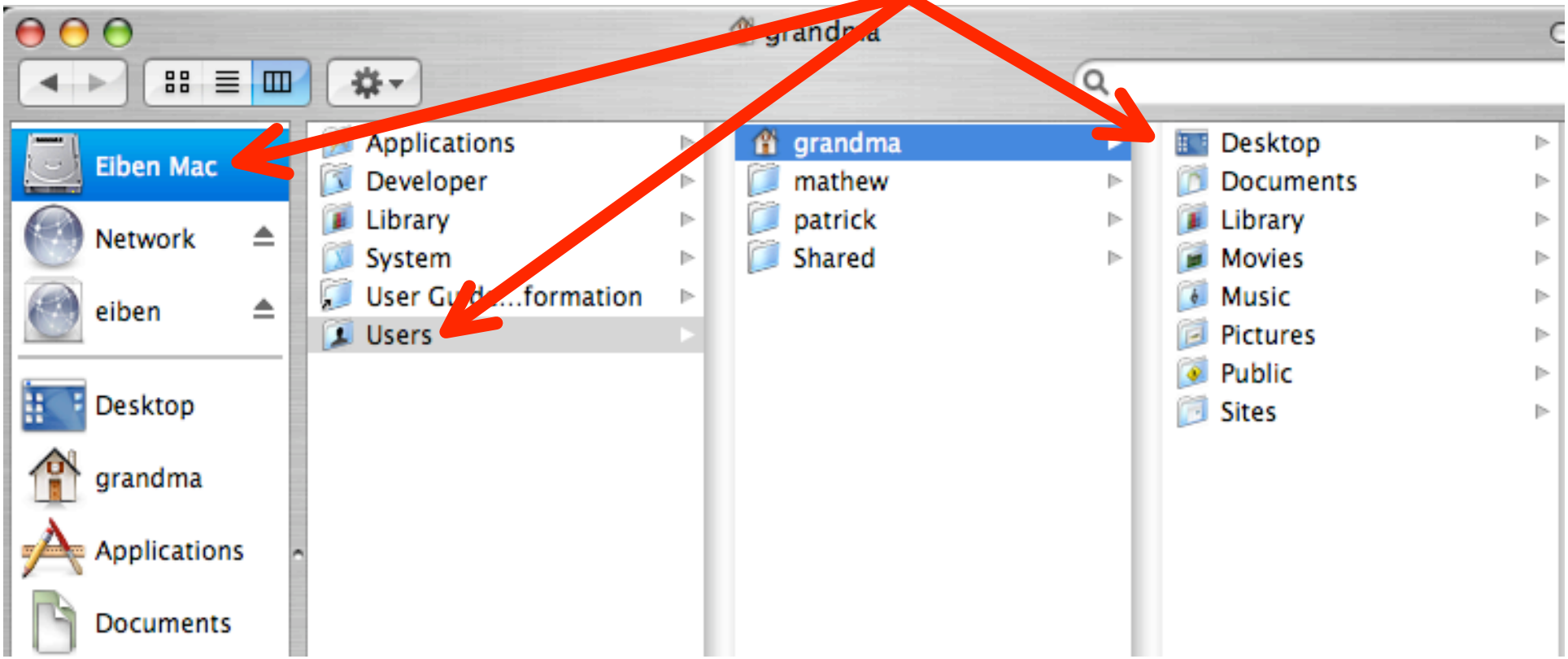
SPYING

You can also know you have a **mobile** account if you get synchronizing windows.



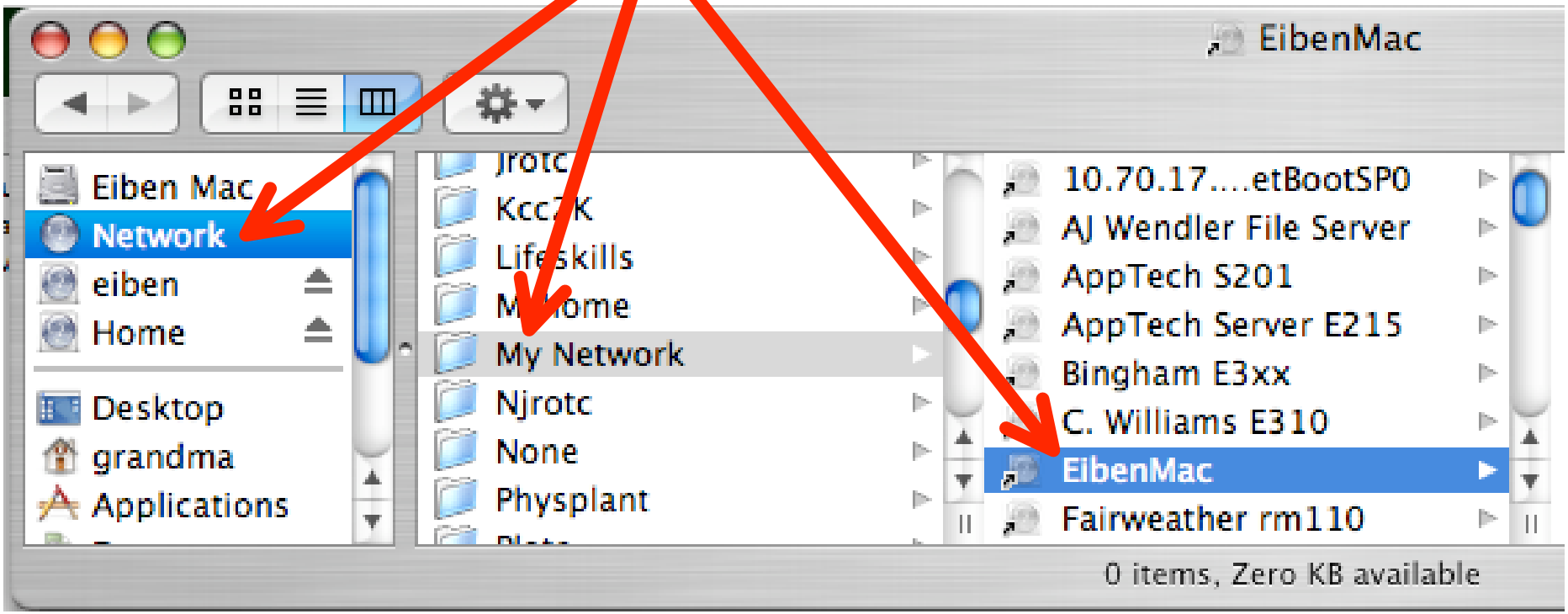
SPYING

If you are logged into your hard drive or have a mobile account, you can see the **hard drive** (left), and trace it through the Users folder to your files on the right. **Always** keep your documents in your **Documents** or **Desktop** folders.



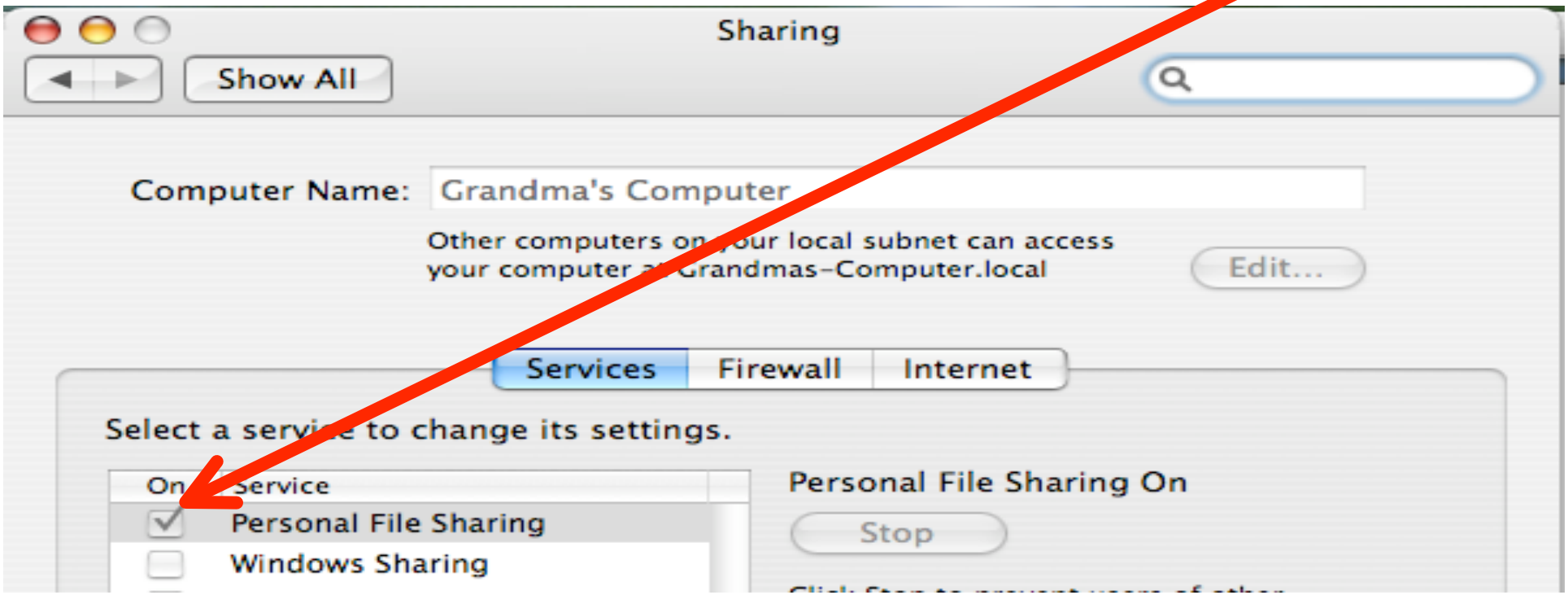
SPYING

Anyone, including students, can locate your computer hard drive by looking in the network. If you have an easy password to guess, they can log onto your computer with full access if you leave **Personal File Sharing activated** in System Preferences.



SPYING

Be very careful about your **password** and what **Sharing** features you turn on. If you have a good password, others can only access your **Public Files** with **Personal File Sharing** (my students use it to turn in their work - it can be useful). Make sure your **Firewall** is on.

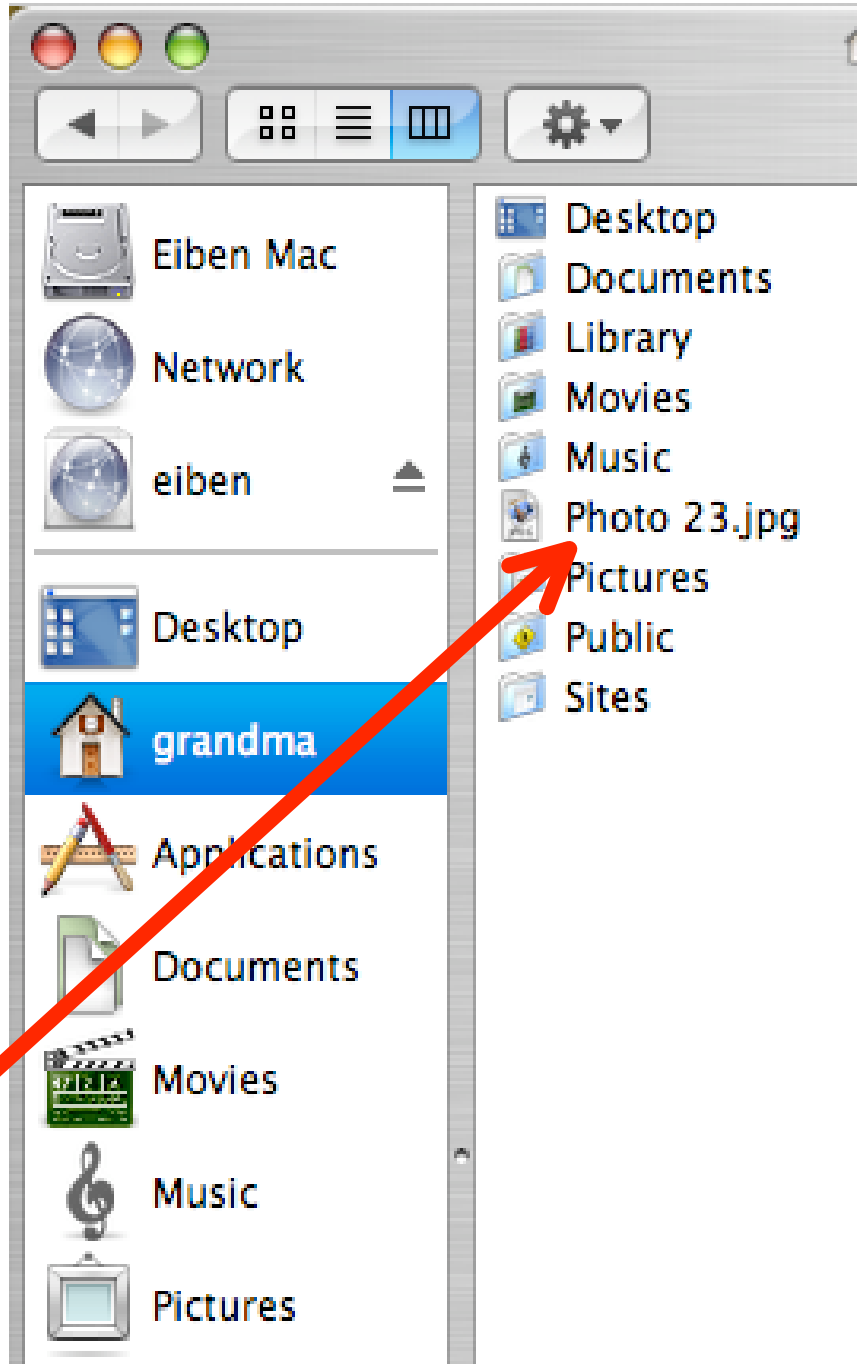


SPYING

If you log into the server (on the network) **or** have a mobile account, you need to take some precautions to make your files safe.

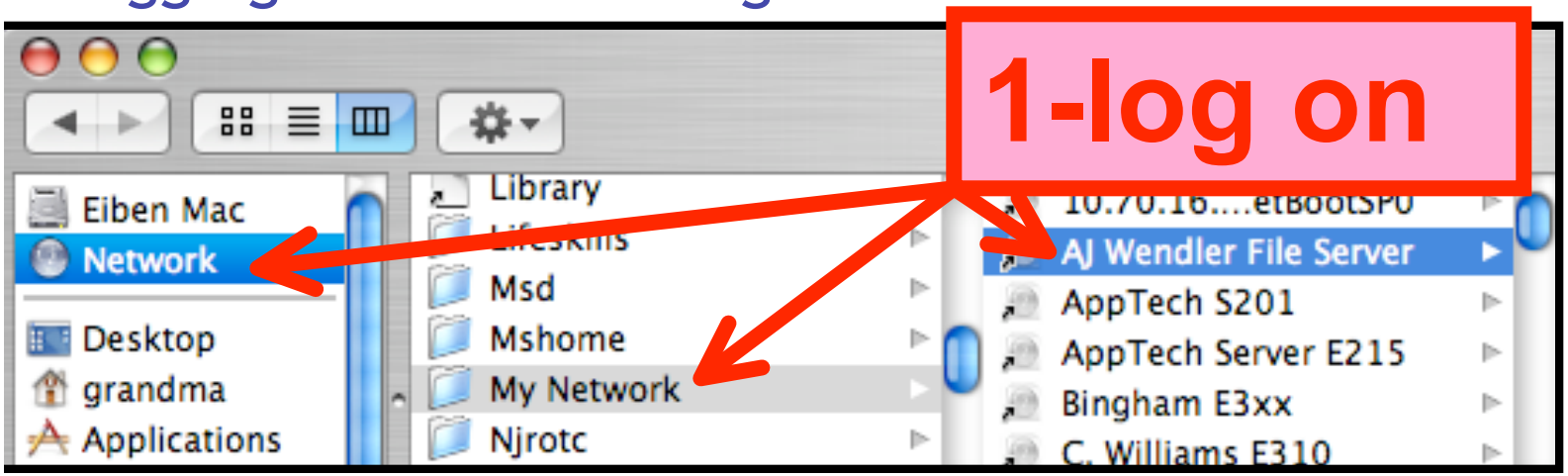
Always make sure your documents are **inside** your **Document** or **Desktop** folders.

Do you see the **unprotected** (**because it is not in a folder**) "Photo 23.jpg" document?



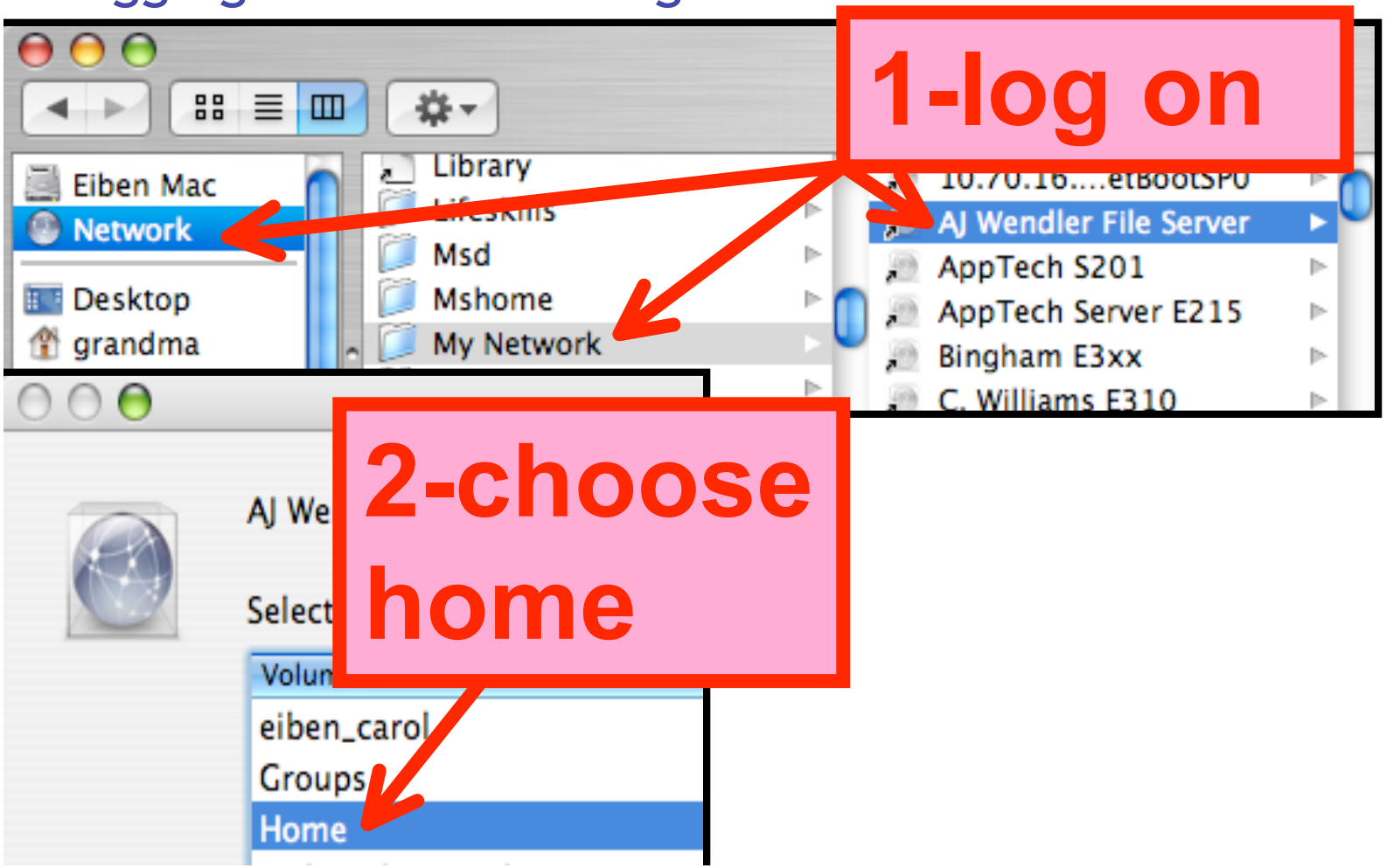
SPYING

Anyone, including students, can locate your **server** file by logging on and choosing the **Home** and **WDStaff** folders.



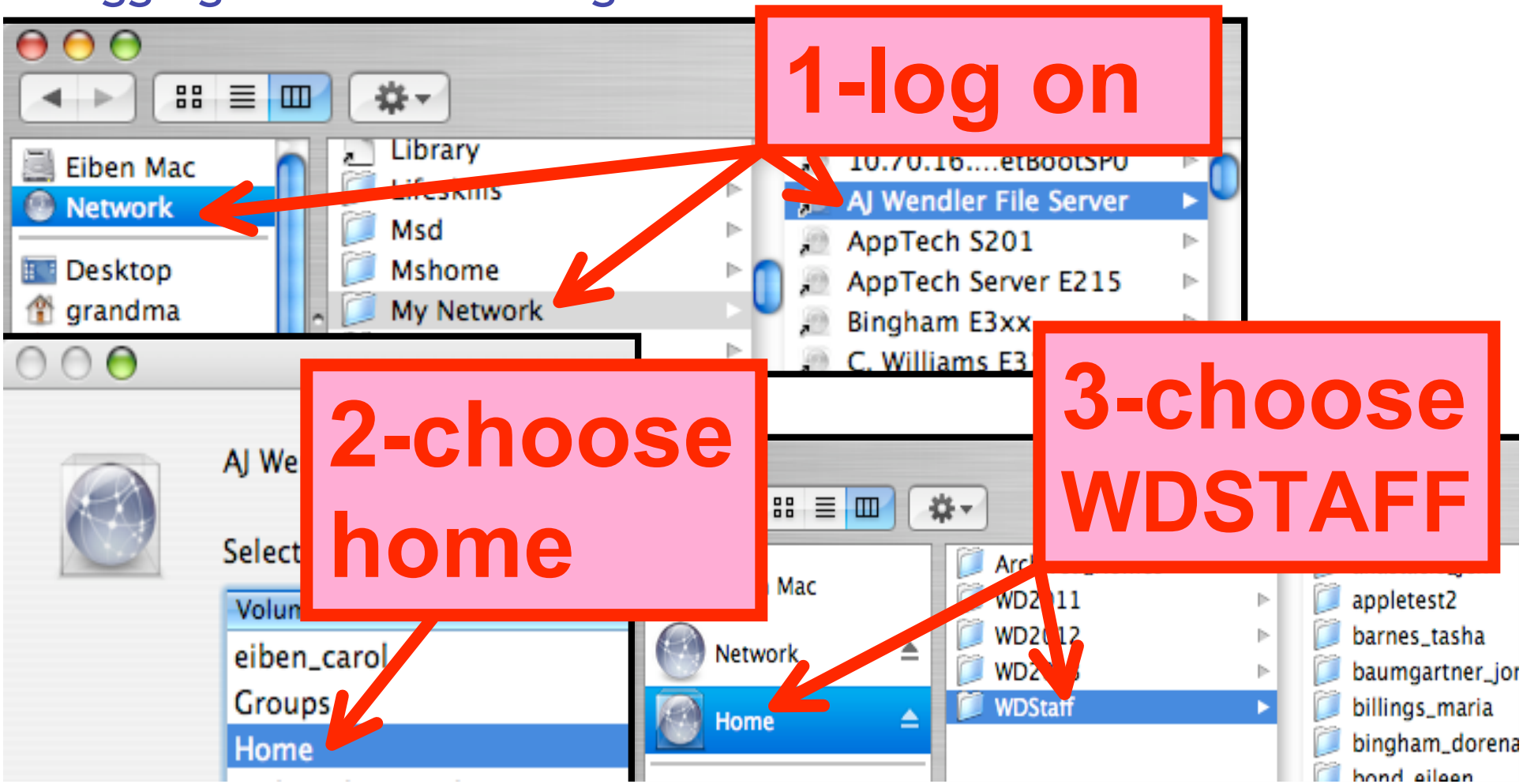
SPYING

Anyone, including students, can locate your **server** file by logging on and choosing the Home and WDStaff folders.



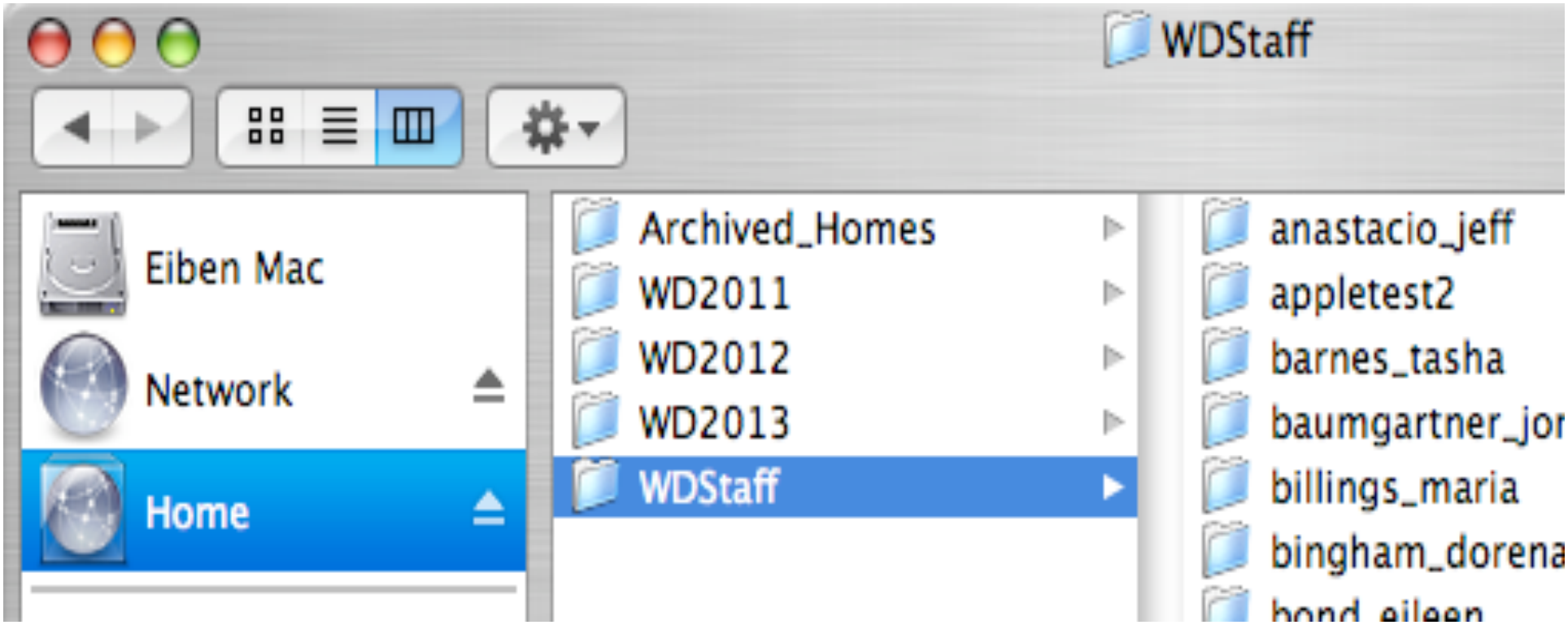
SPYING

Anyone, including students, can locate your **server** file by logging on and choosing the **Home** and **WDStaff** folders.



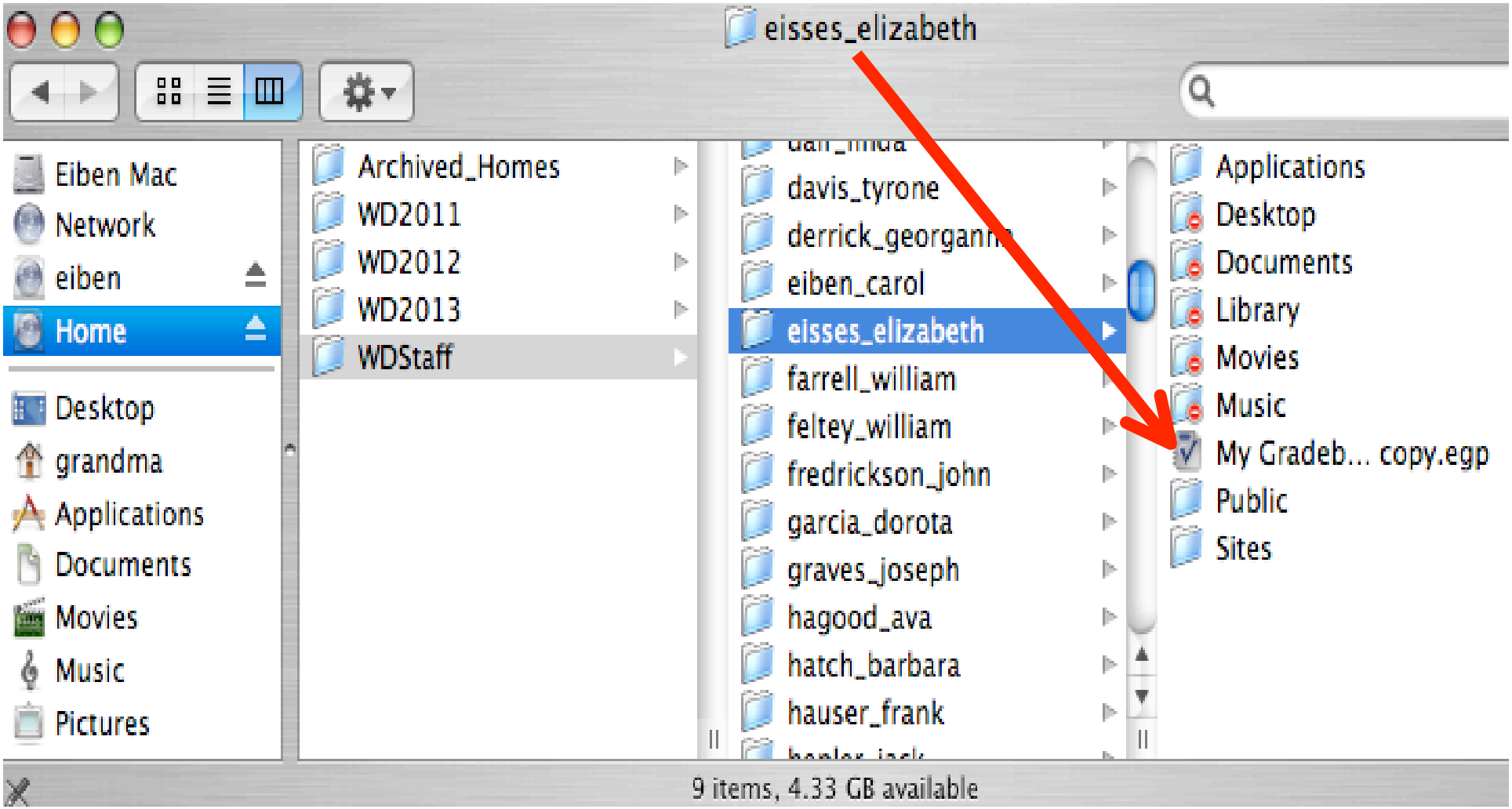
SPYING

Laptop teams turn their work into the **WDStaff** folders, so they look at your server folder **every day**!



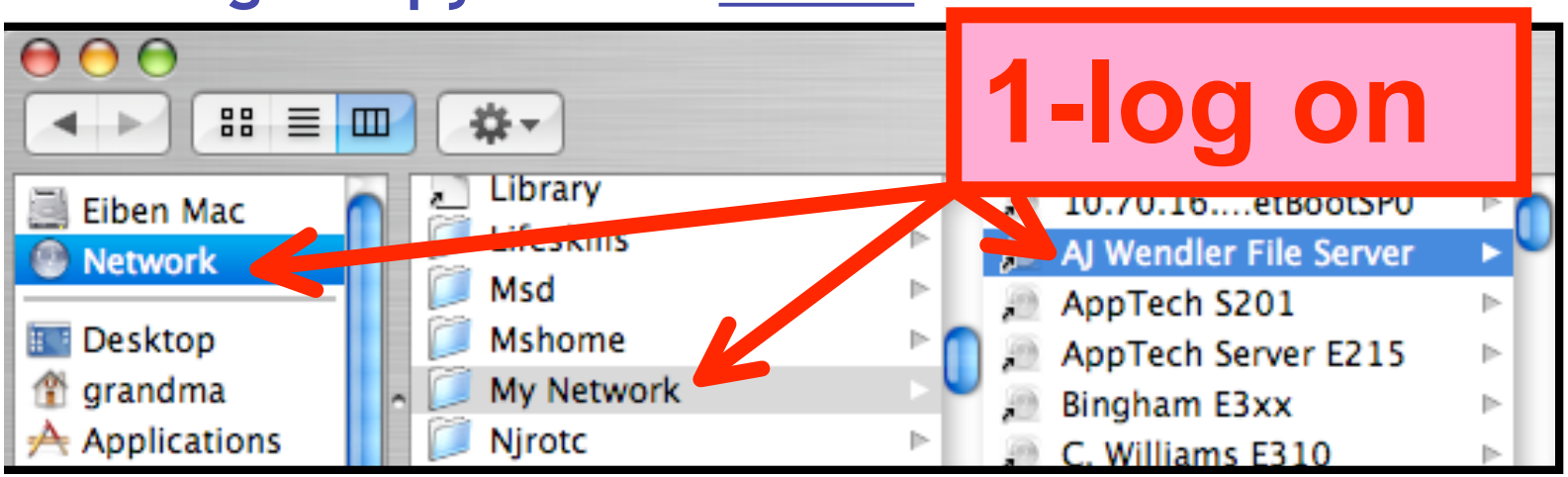
SPYING

Look what Betsy forgot in her folder on the server…



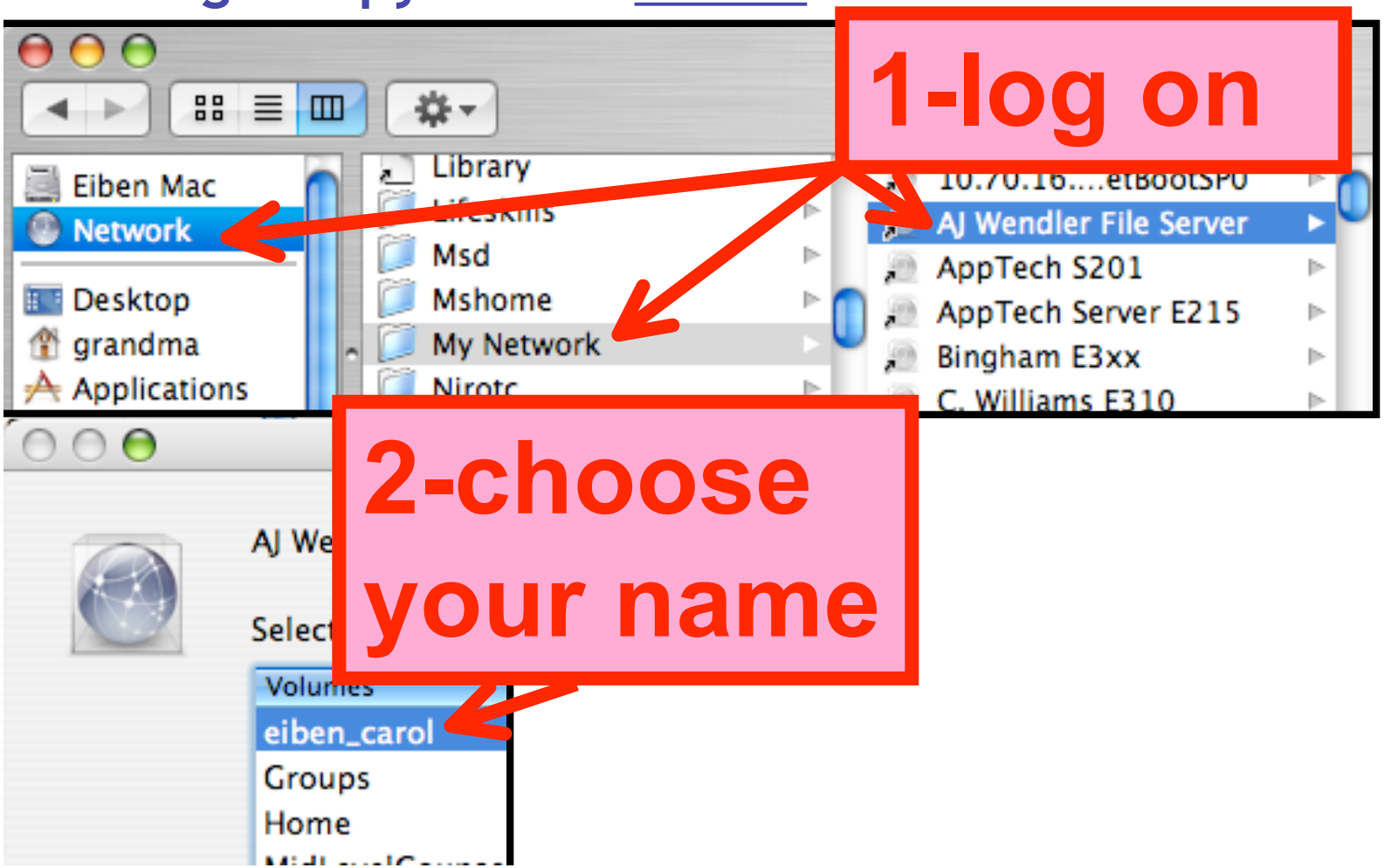
SPYING

Always save your documents in a locked folder when saving a copy on the server…



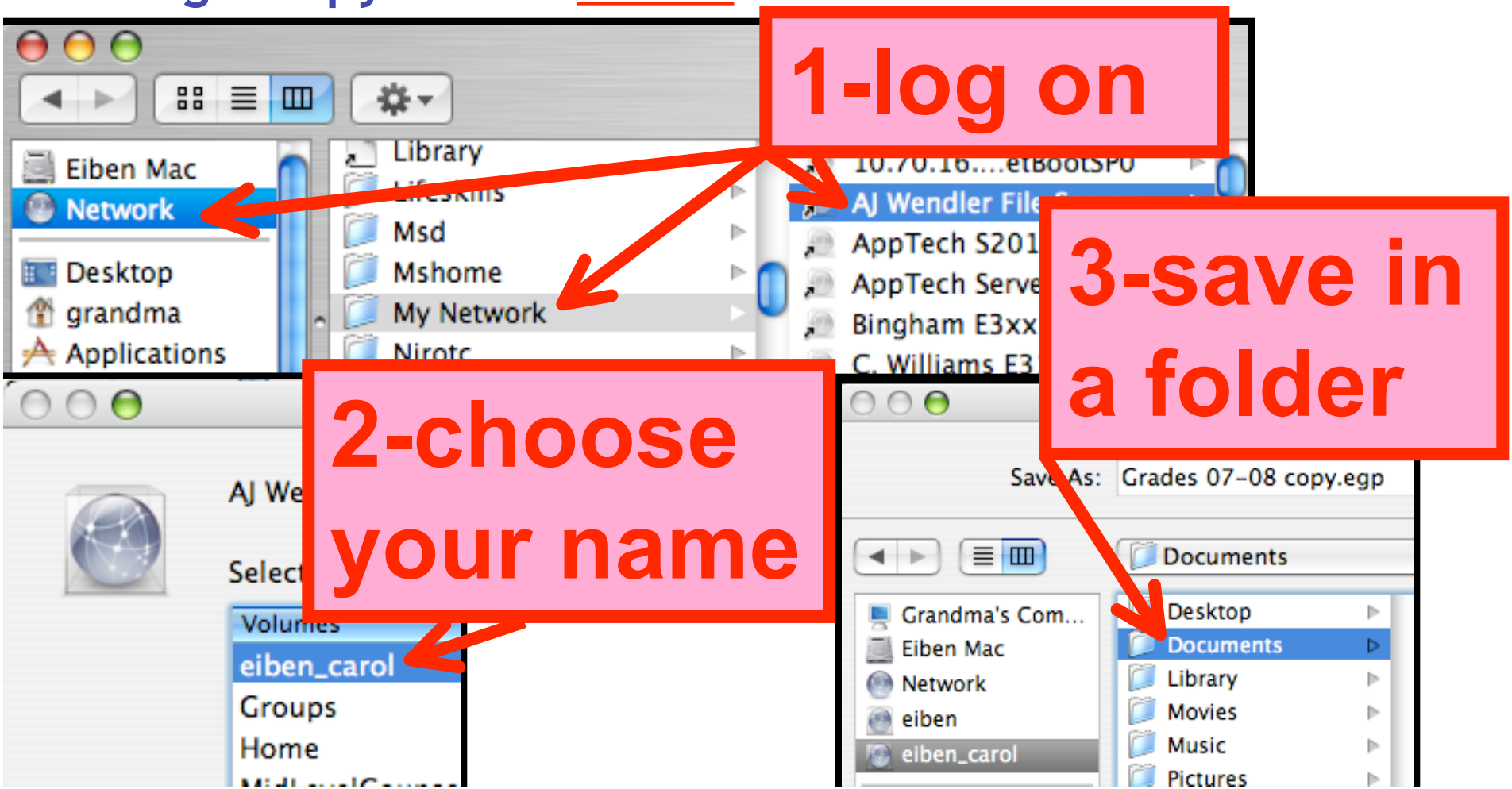
SPYING

Always save your documents in a locked folder when saving a copy on the server…



SPYING

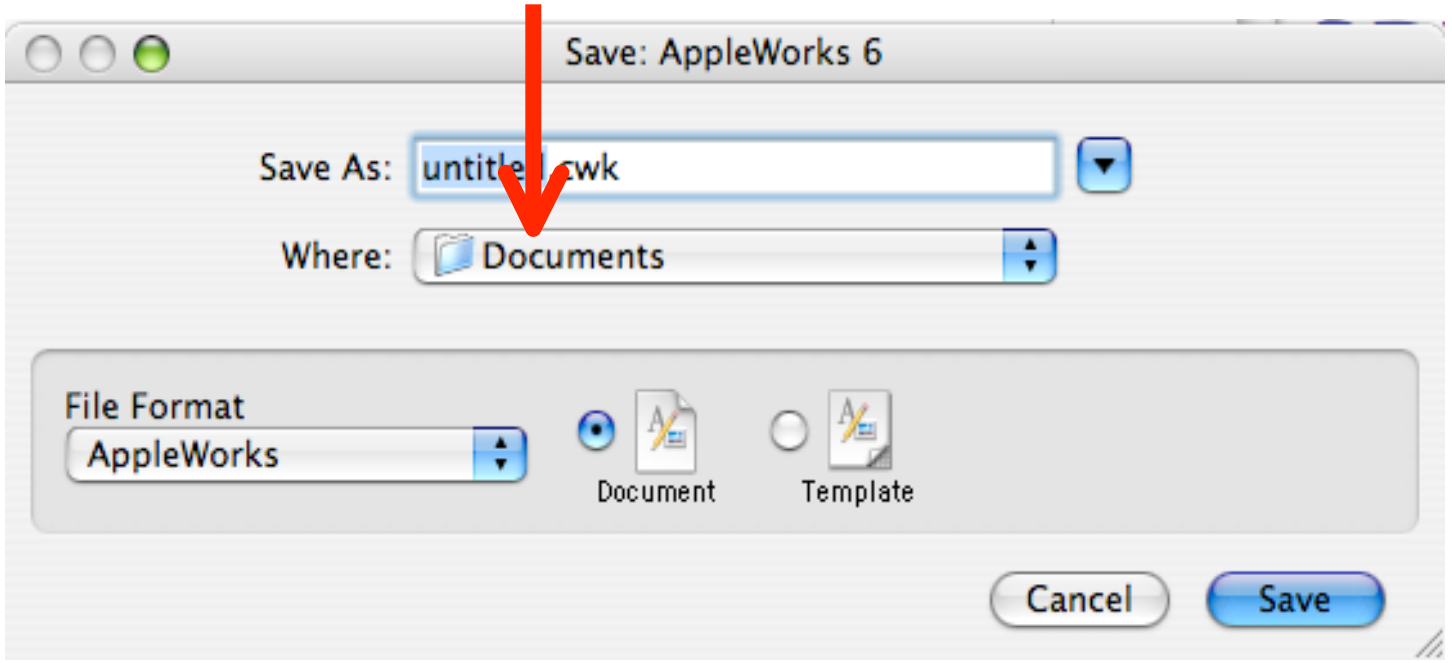
Always save your documents in a locked folder when saving a copy on the server…



SPYING

If you have a mobile account, a copy is automatically saved on your hard drive AND on the server, so you do not have to log onto the server to save a copy.

Just make sure to always save your documents inside your Desktop or Documents folders.



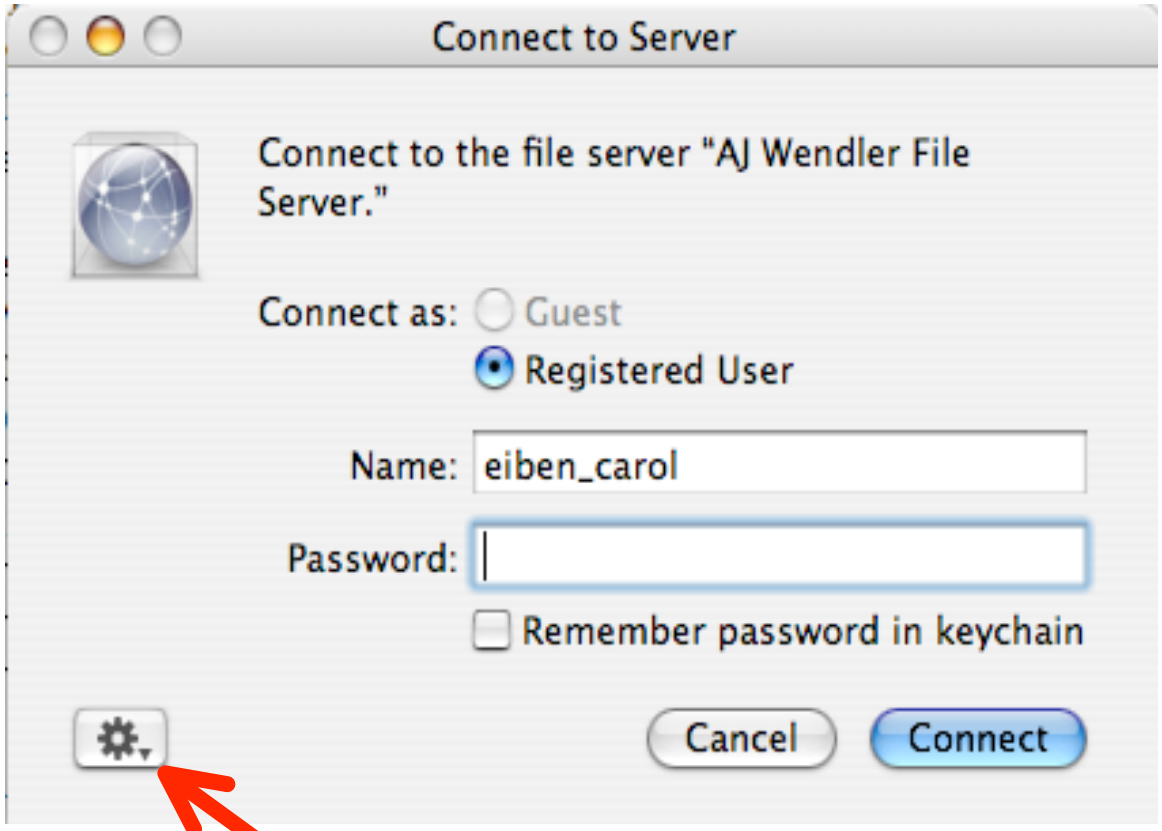
SPYING

Make sure your **password** for the **server** is not obvious.

NEVER

use your

LAST NAME.

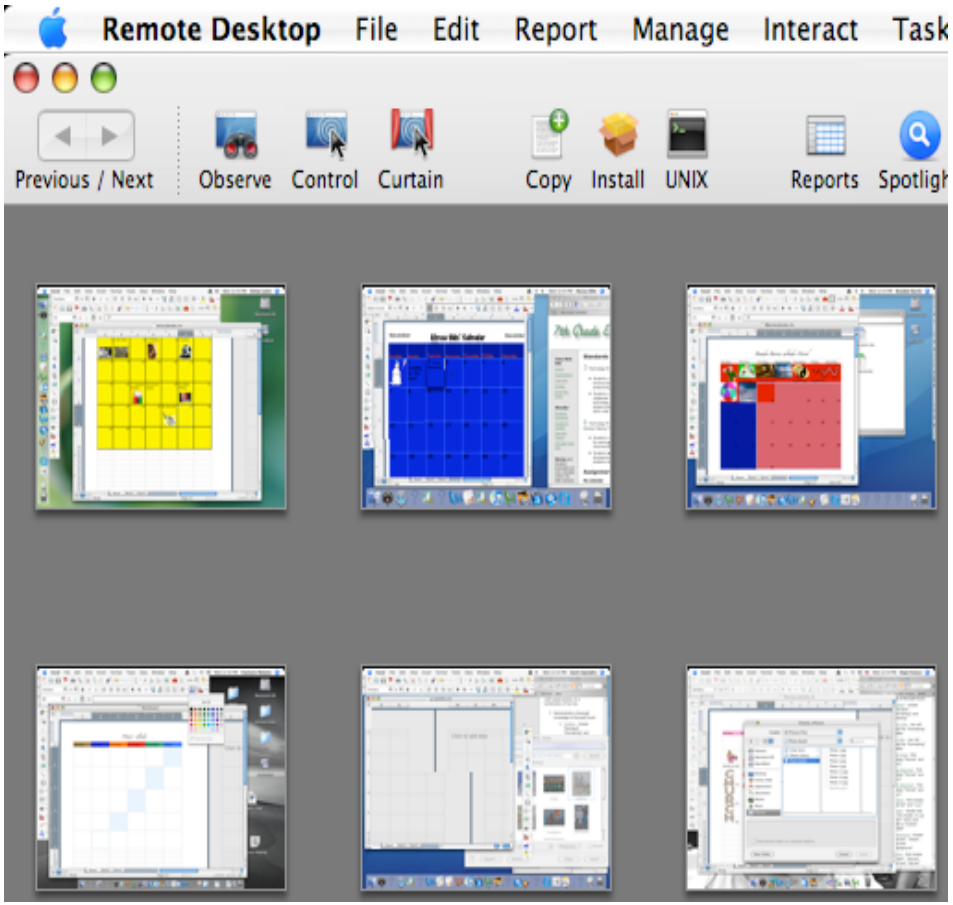


Students are smart enough to figure that out, and get full access to all your files.

Change your password here.

SPYING

Did you know that staff with an administrative password to your computer and Apple Remote Desktop (ARD) software can see and control your screen and all that you do from their own computer?

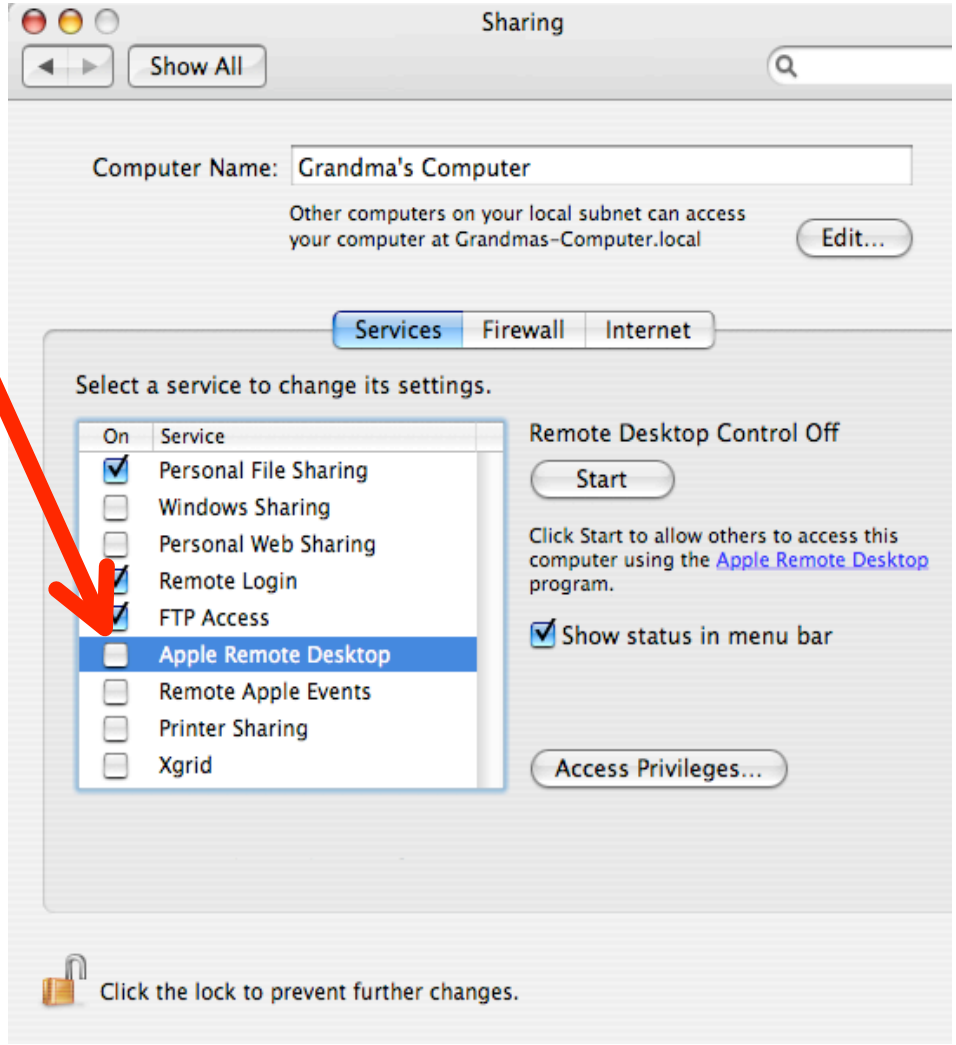


We have ARD so that our Tech Guy can fix your computer remotely, so it can be a very good thing.

All laptop team teachers and computer lab teachers have ARD on their computers, to manage student computers.

SPYING

You can turn Apple Remote Desktop on or off in System Preferences, under "Sharing"



SPYING

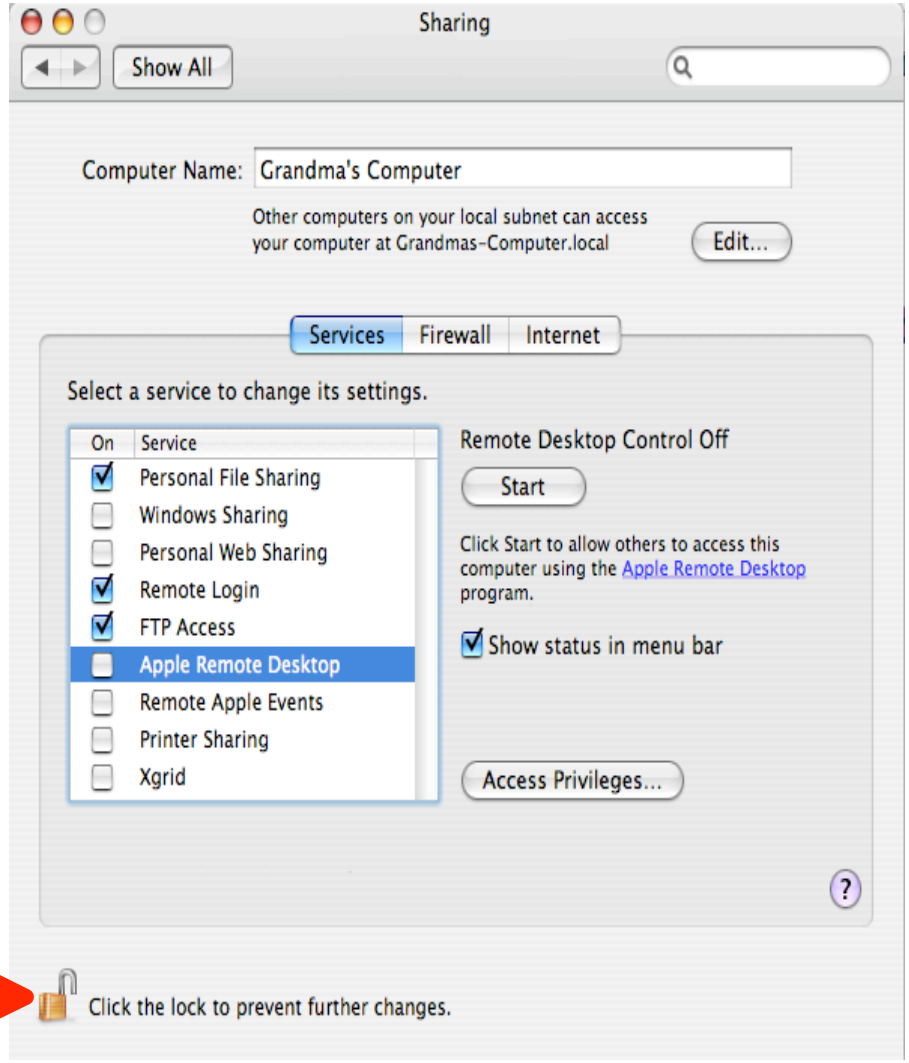
You can turn Apple Remote Desktop on or off in System Preferences, under "Sharing"

You can also see when ARD is active, by putting the binoculars on your menu bar. They are black when active, and grey when inactive.

SPYING

Other options to log onto your computer are available through System Preferences and Sharing too. Click on each option to read what it allows you (and others) to do.

They can be password protected (using your log in password),so if you use these features pick a secure password that is not easily guessed.



SPYING

On the front page of the ASD website is easy access to Webmail.

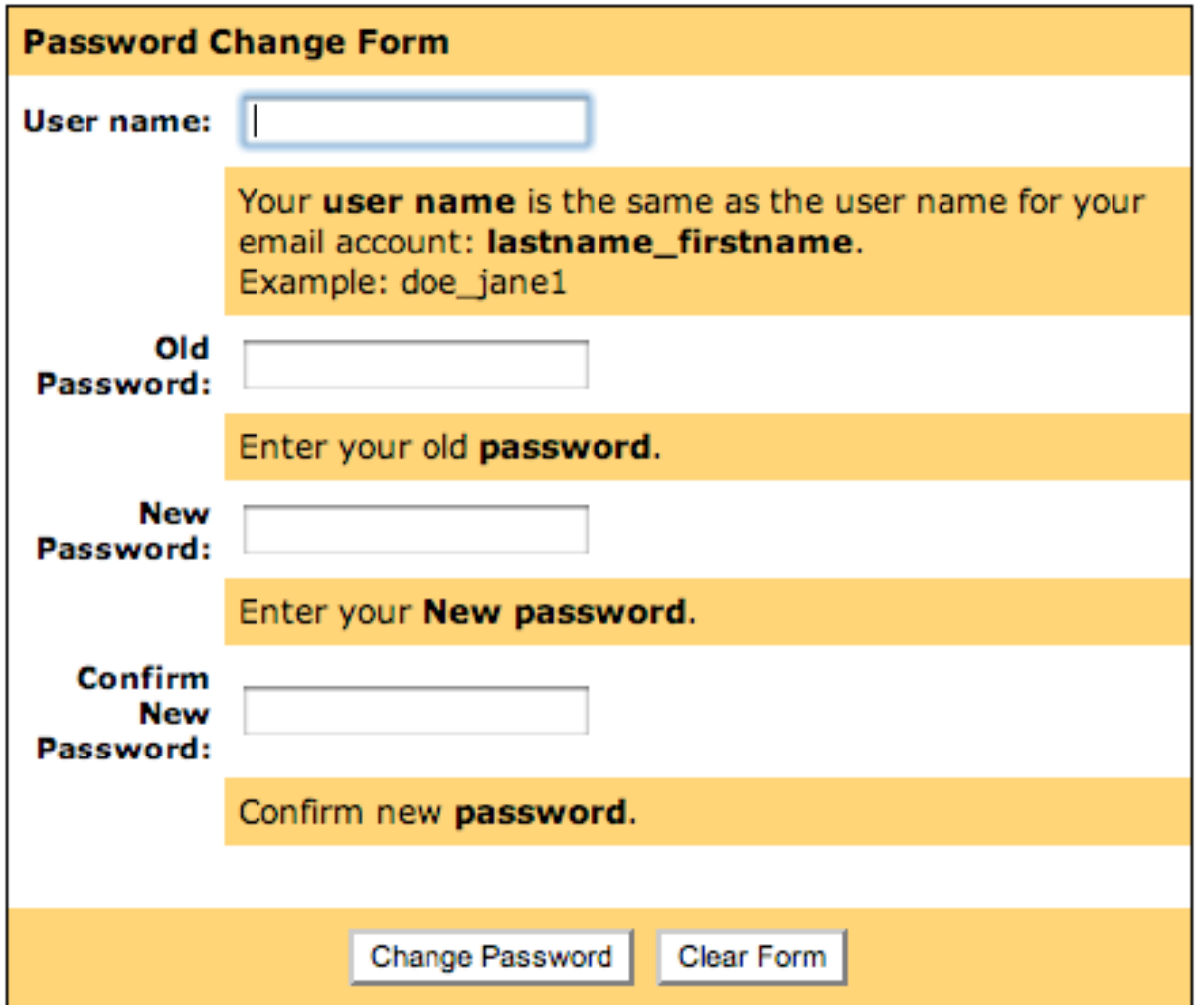
What is your email password?

Need I say more?

SPYING

http://webmail.asdk12.org/chgpassword

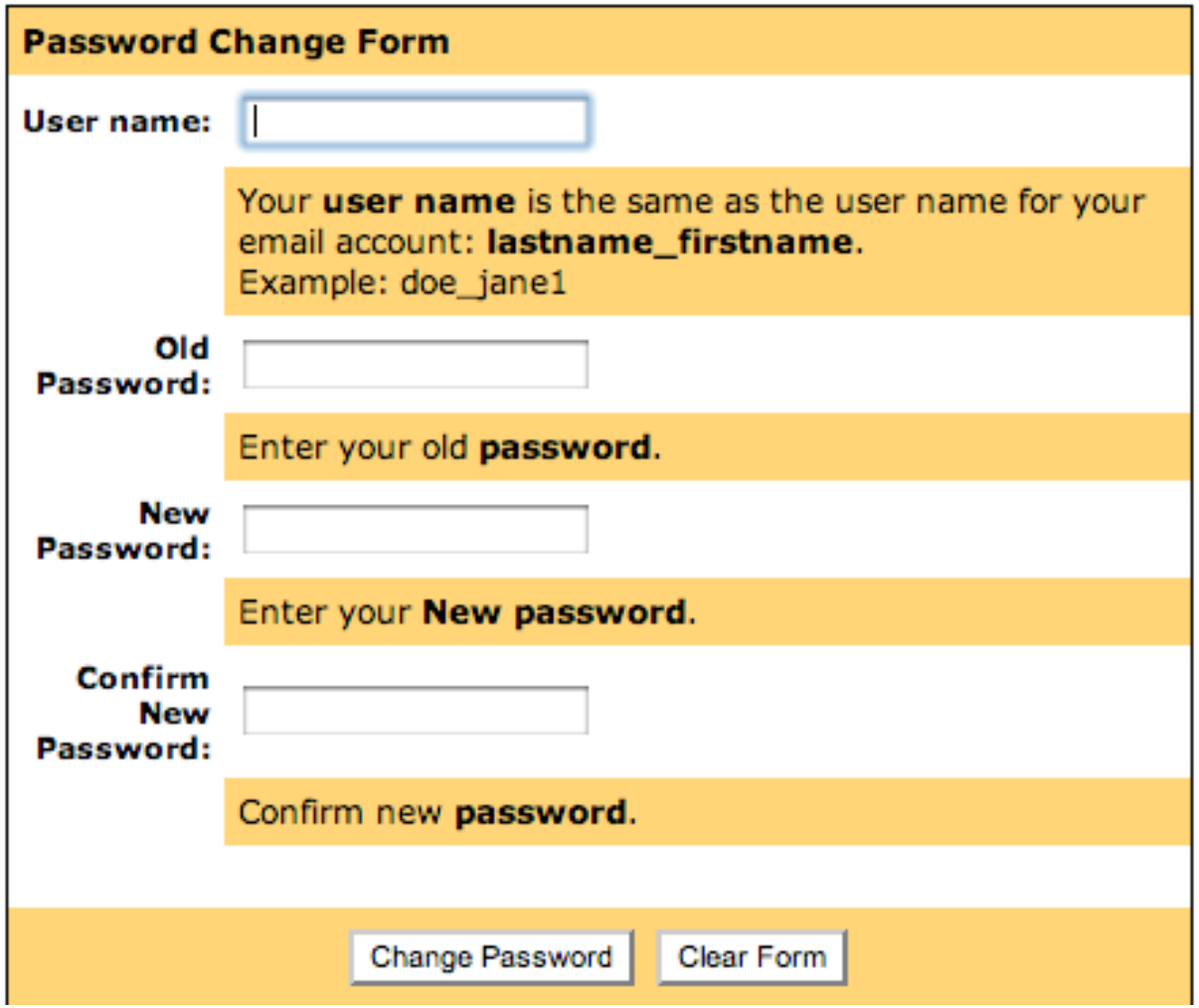
Change your email password here.



SPYING

http://webmail.asdk12.org/chgpassword

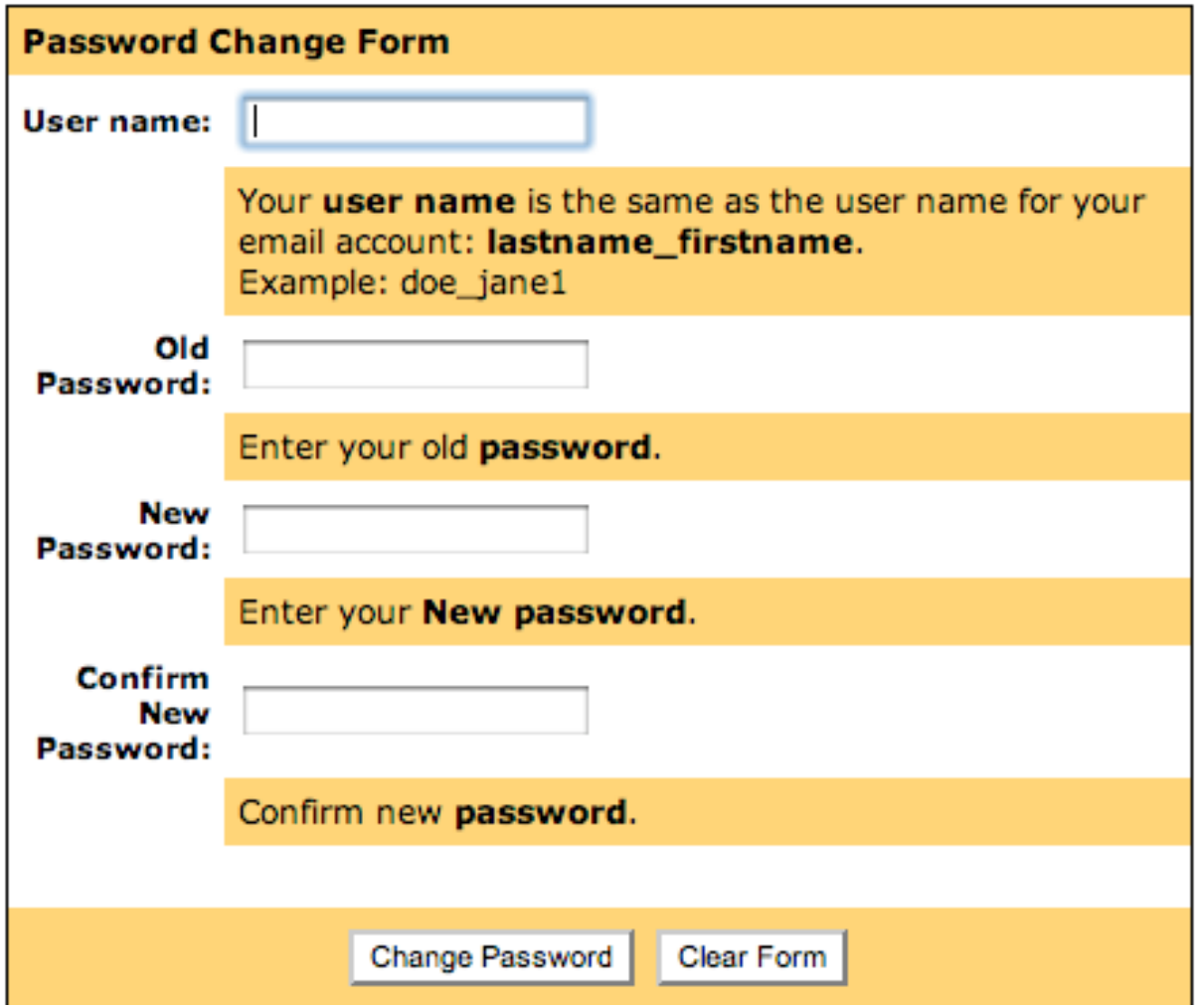
This will also change your District Connection password.



SPYING

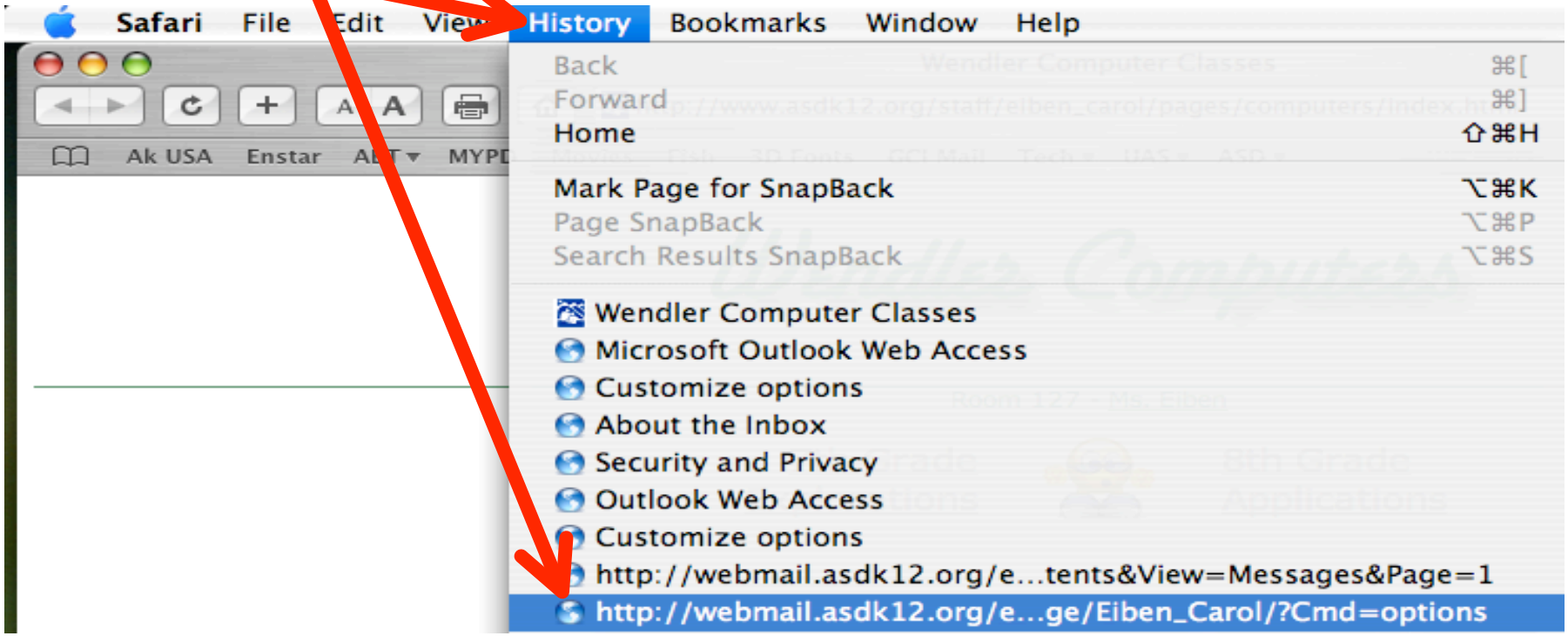
http://webmail.asdk12.org/chgpassword

This will NOT change your Fetch password.



SPYING

If you use Webmail, **always** Quit your browser (Safari) or clear your Cache when you are done, or someone can come in behind you and easily access your emails under "History" without even entering a password!



SPYING

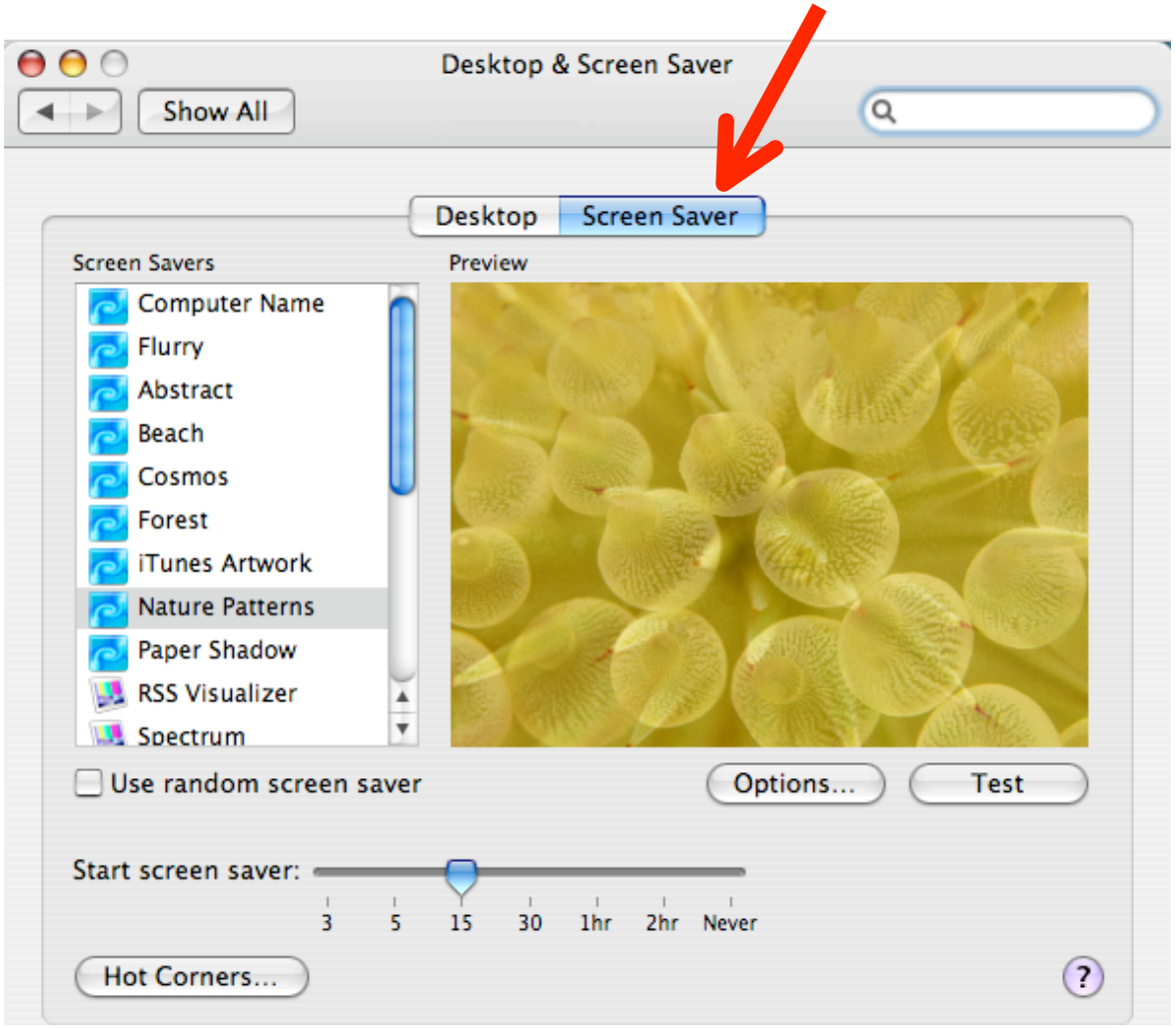
Do students walk up to your desk and look over your shoulder at your computer screen?

Do you walk away from your computer and leave it on, so that others could look at confidential information?

Would you like to make your computer more secure without having to log off or turn it off?

SPYING

1. Use a Screen Saver (System Preferences).



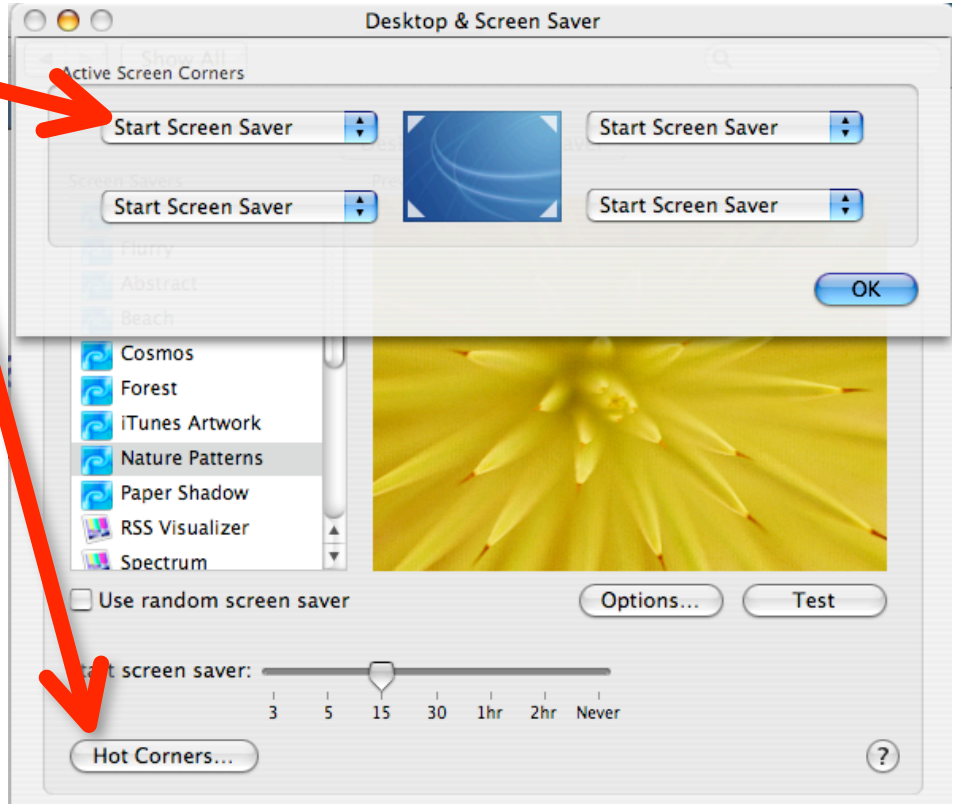
SPYING

1. Use a Screen Saver (System Preferences).
2. Make it require a password to turn it off (Security in System Preferences).

Security
Show All
FileVault
FileVault secures your home folder by encrypting its contents. It automatically encrypts and decrypts your files while you're using them.
WARNING: Your files will be encrypted using your login password. If you forget your login password and you don't know the master password, your data will be lost.
A master password is not set for this computer.
This is a "safety net" password. It lets you unlock any FileVault account on this computer.
Set Master Password...
FileVault protection is off for this account.
Turning on FileVault may take a while.
Turn On FileVault...
Require password to wake this computer from sleep or screen saver

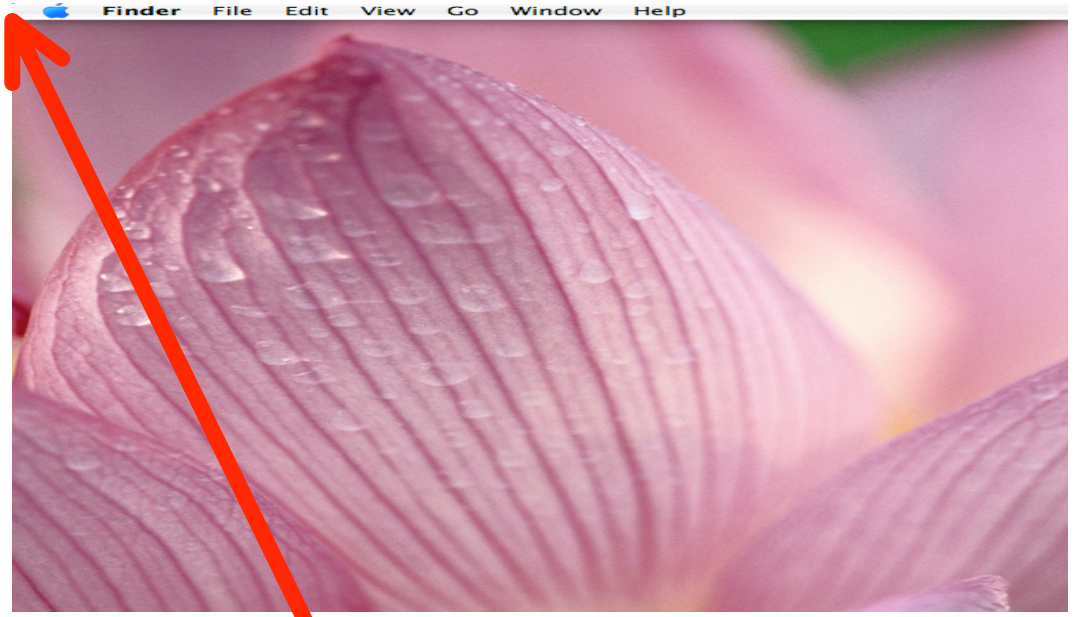
SPYING

1. Use a Screen Saver (System Preferences).
2. Make it require a password to turn it off (Security in System Preferences).
3. Use Hot Corners to activate it immediately (in the Screen Saver window).



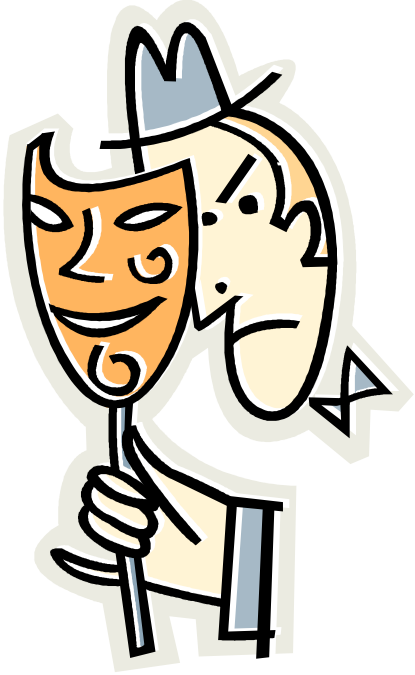
SPYING

1. Use a Screen Saver (System Preferences).
2. Make it require a password to turn it off (Security in System Preferences).
3. Use Hot Corners to activate it immediately (in the Screen Saver window).
4. Touch a corner with a mouse to activate it.



Another security problem can happen with:

Junk Emails



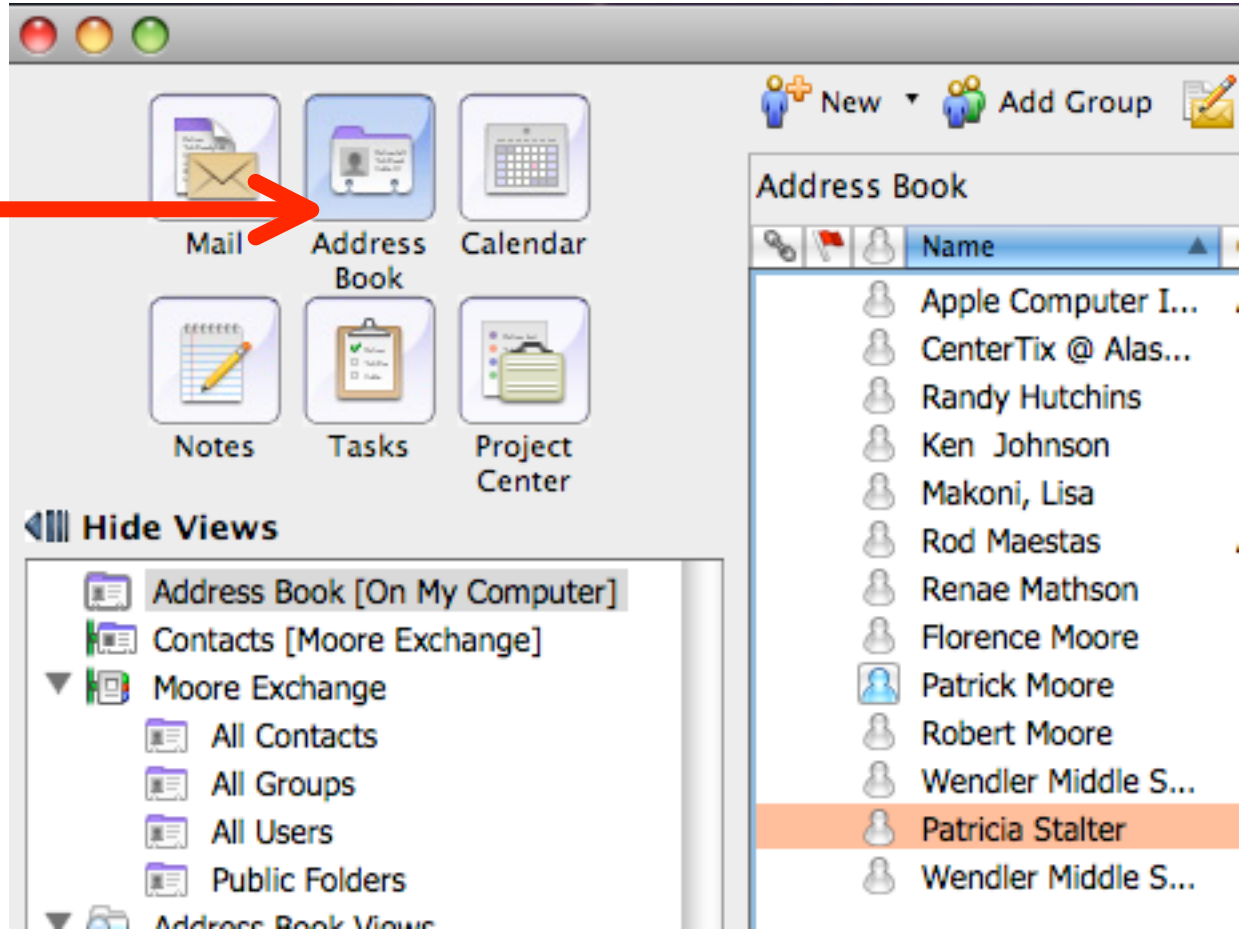
JUNK MAIL

Remember this?

JUNK MAIL

You can fix address problems like this:

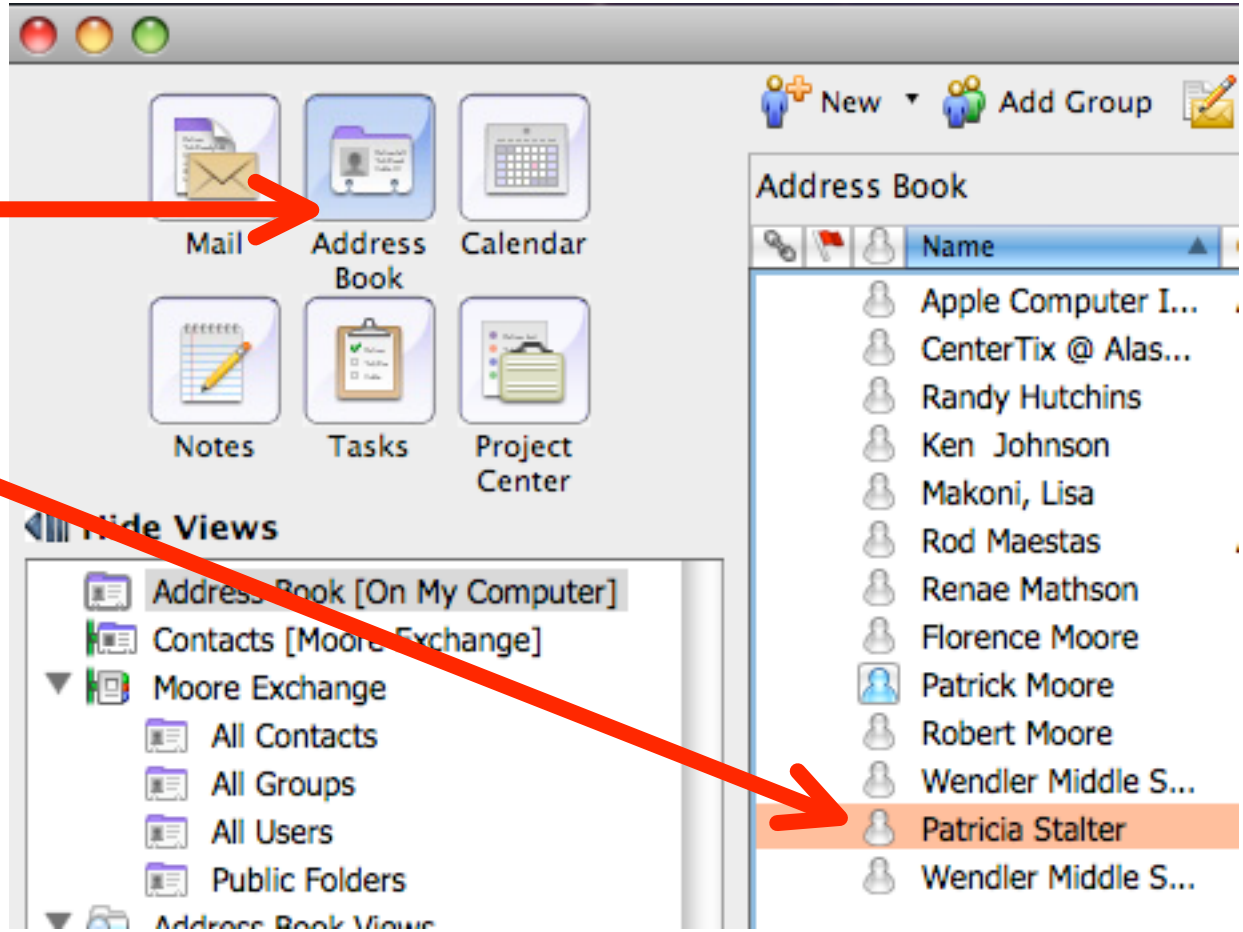
1. Choose Address Book.



JUNK MAIL

You can fix address problems like this:

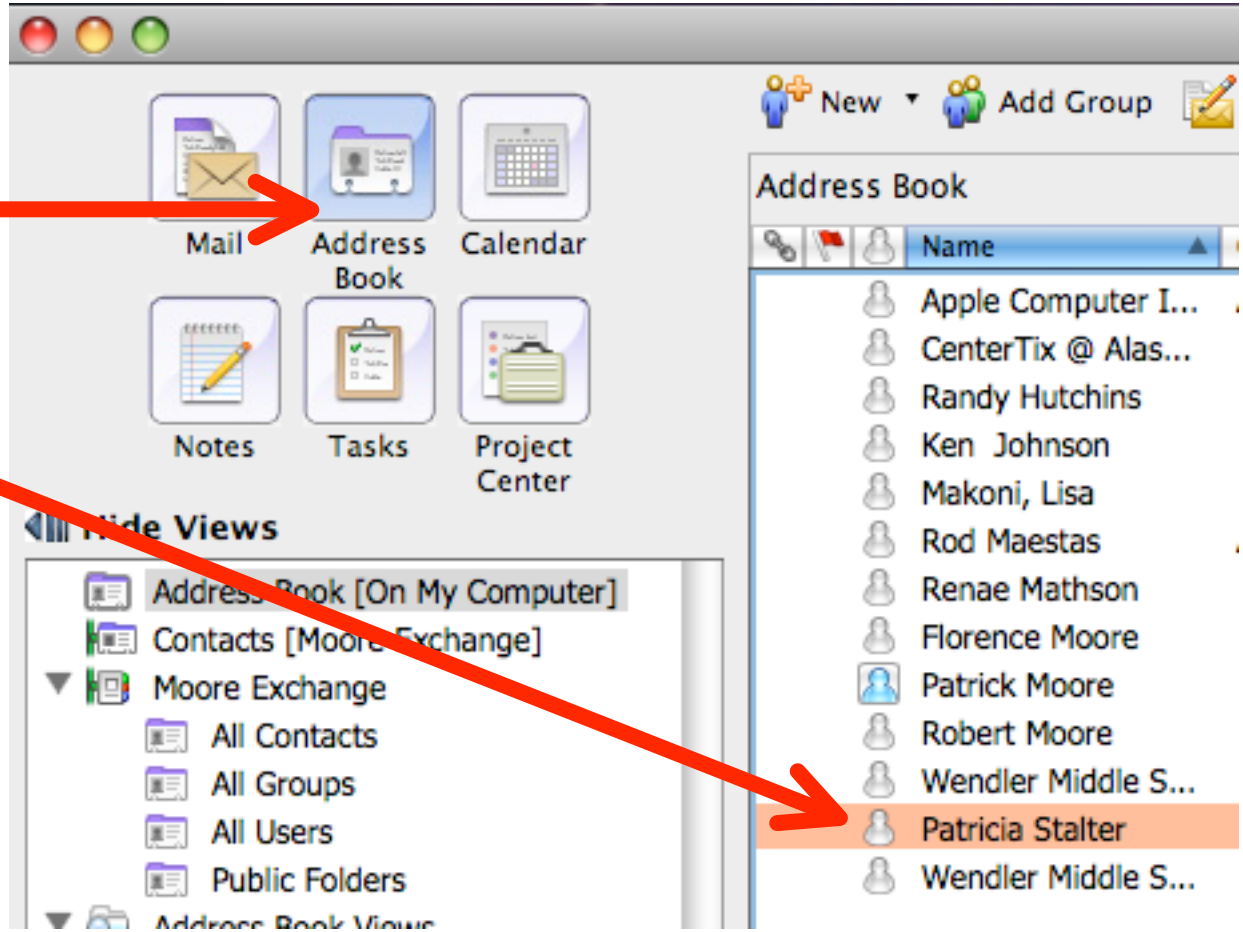
1. Choose Address Book.
2. Highlight the address.



JUNK MAIL

You can fix address problems like this:

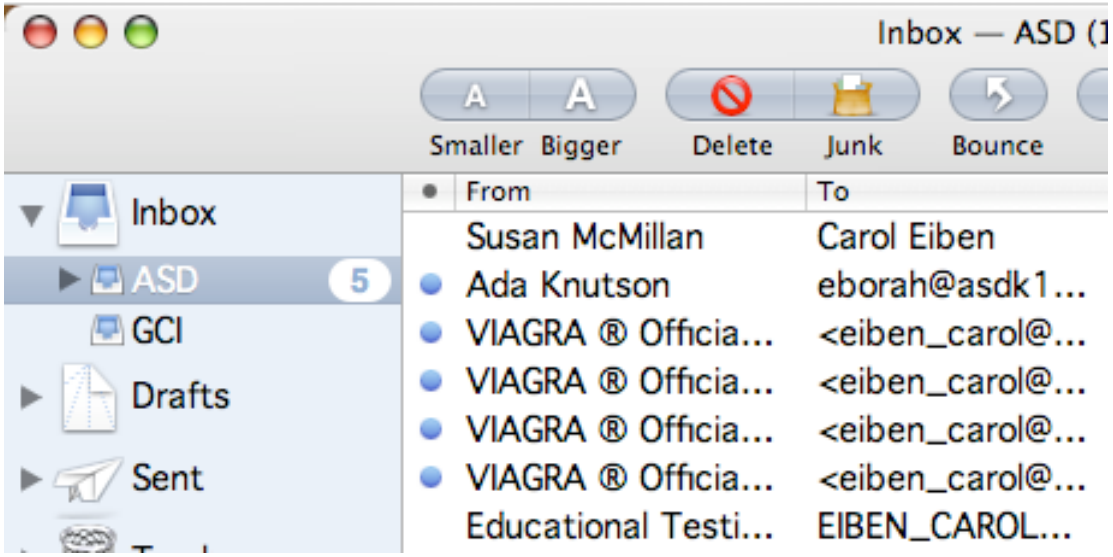
1. Choose Address Book.
2. Highlight the address.
3. Press "delete" key or drag it to the trash.



JUNK MAIL

Prevention is preferable.

1. NEVER open junk mail!

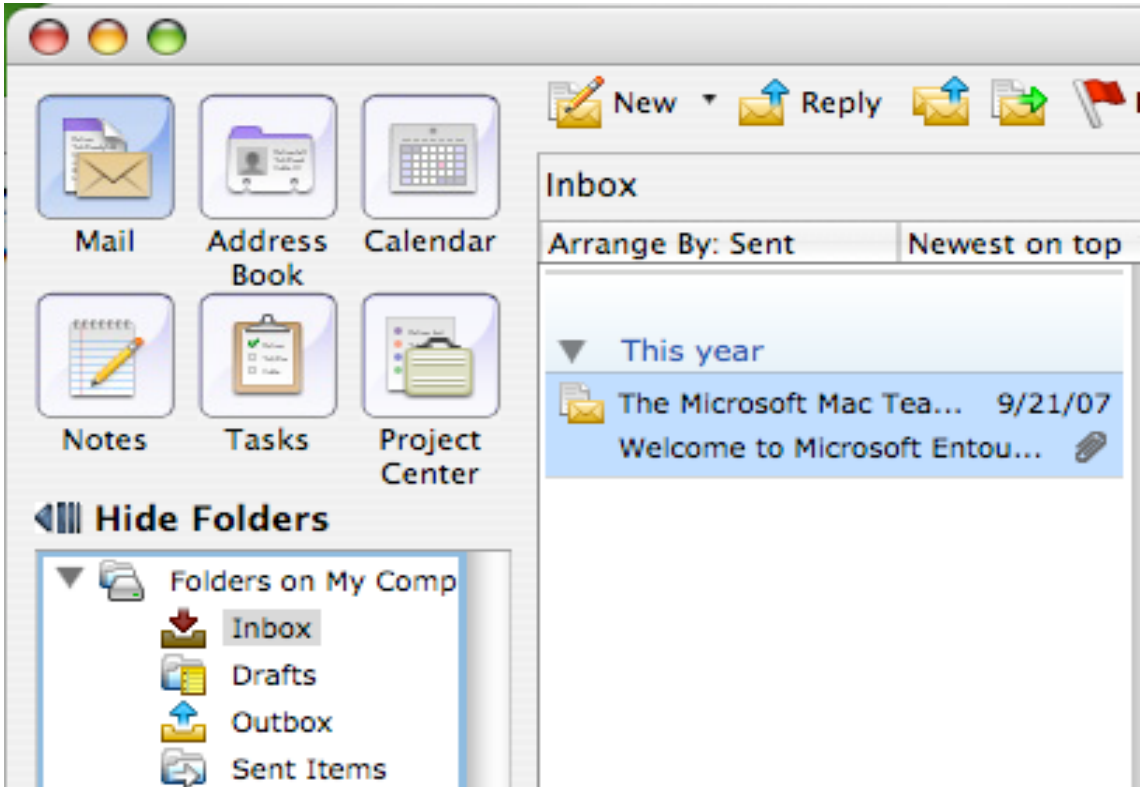


Opening sends a message to the sender that you are there - and they will send MORE!

JUNK MAIL

Prevention is preferable.

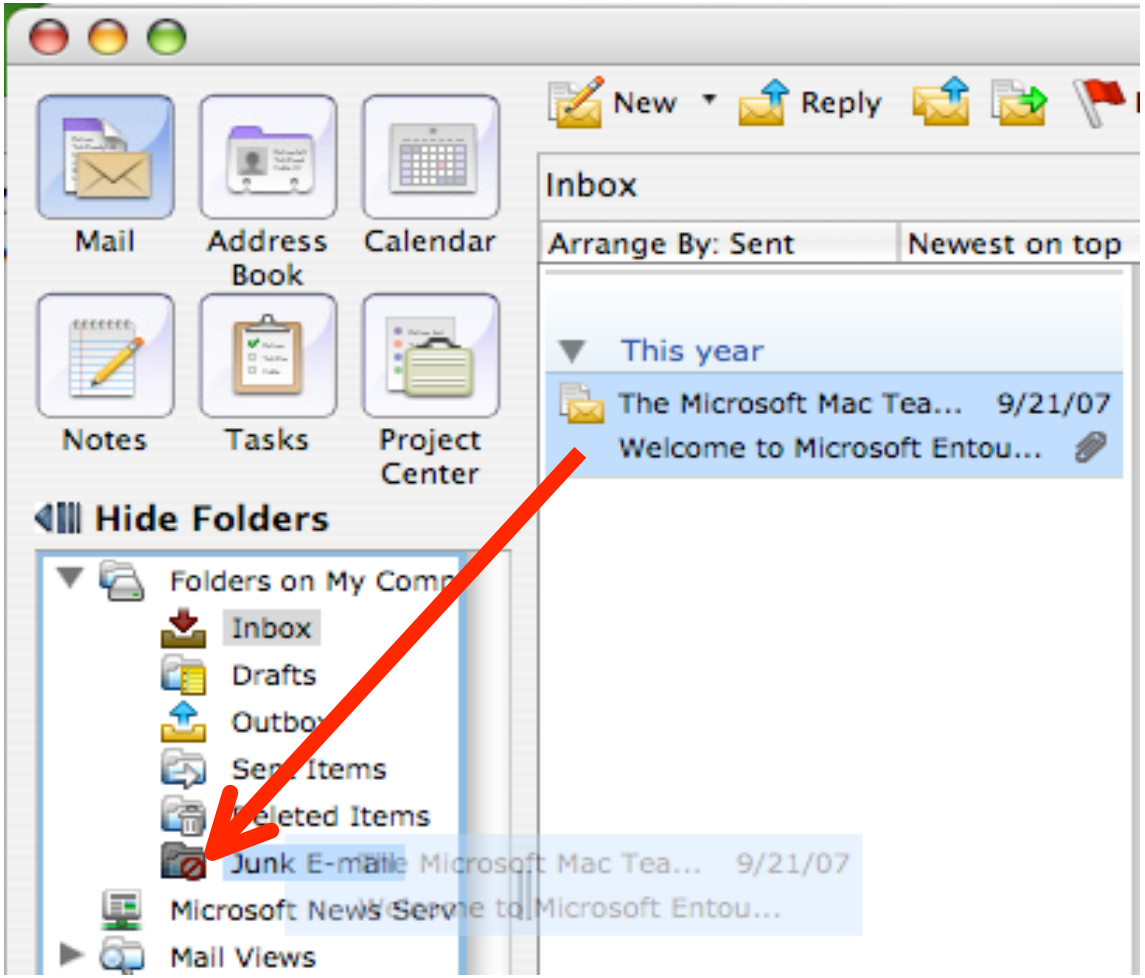
2. When another email is open, **select** the junk mail (hold the Apple key down).



JUNK MAIL

Prevention is preferable.

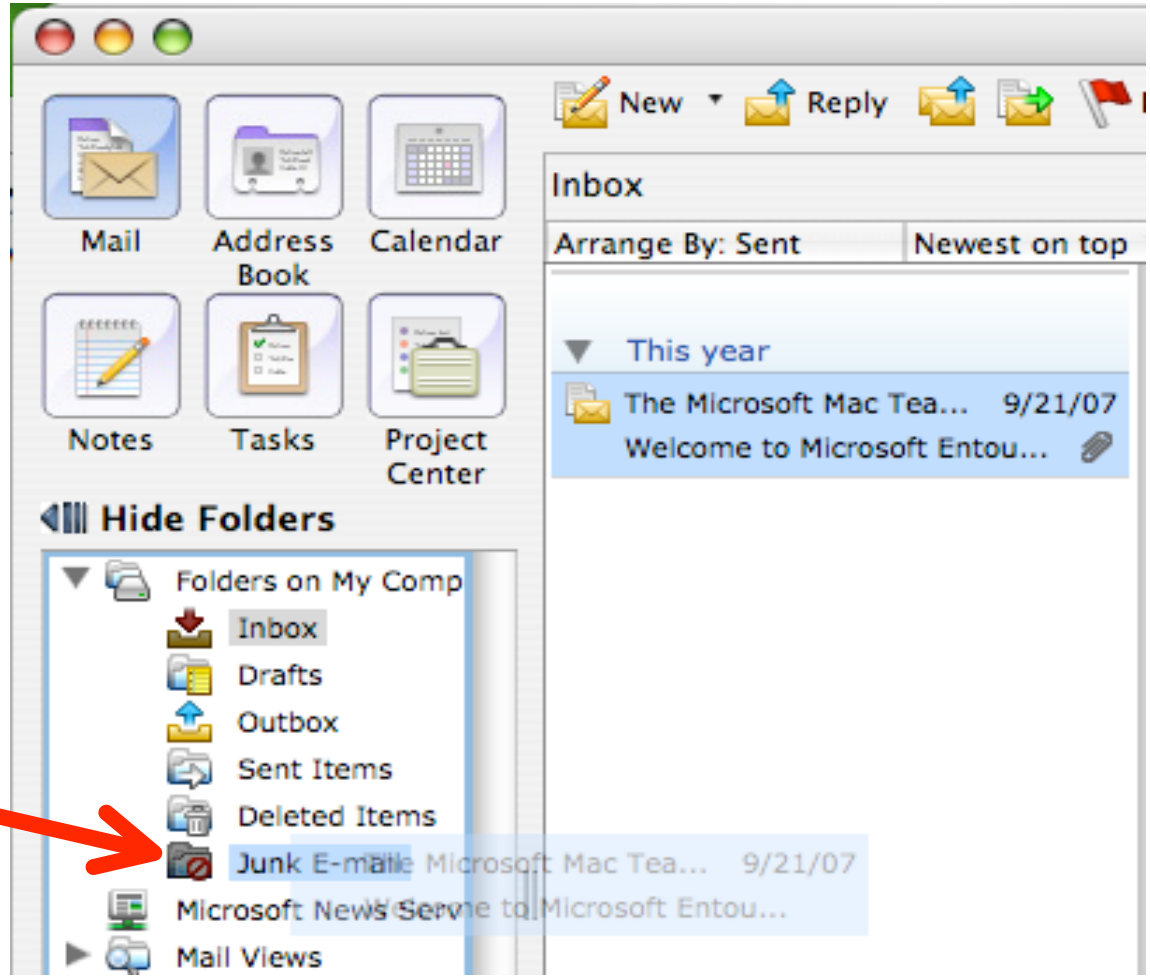
2. When another email is open, **select** the junk mail (hold the Apple key down).
3. Drag it with your mouse to the **junk mail folder**.



JUNK MAIL

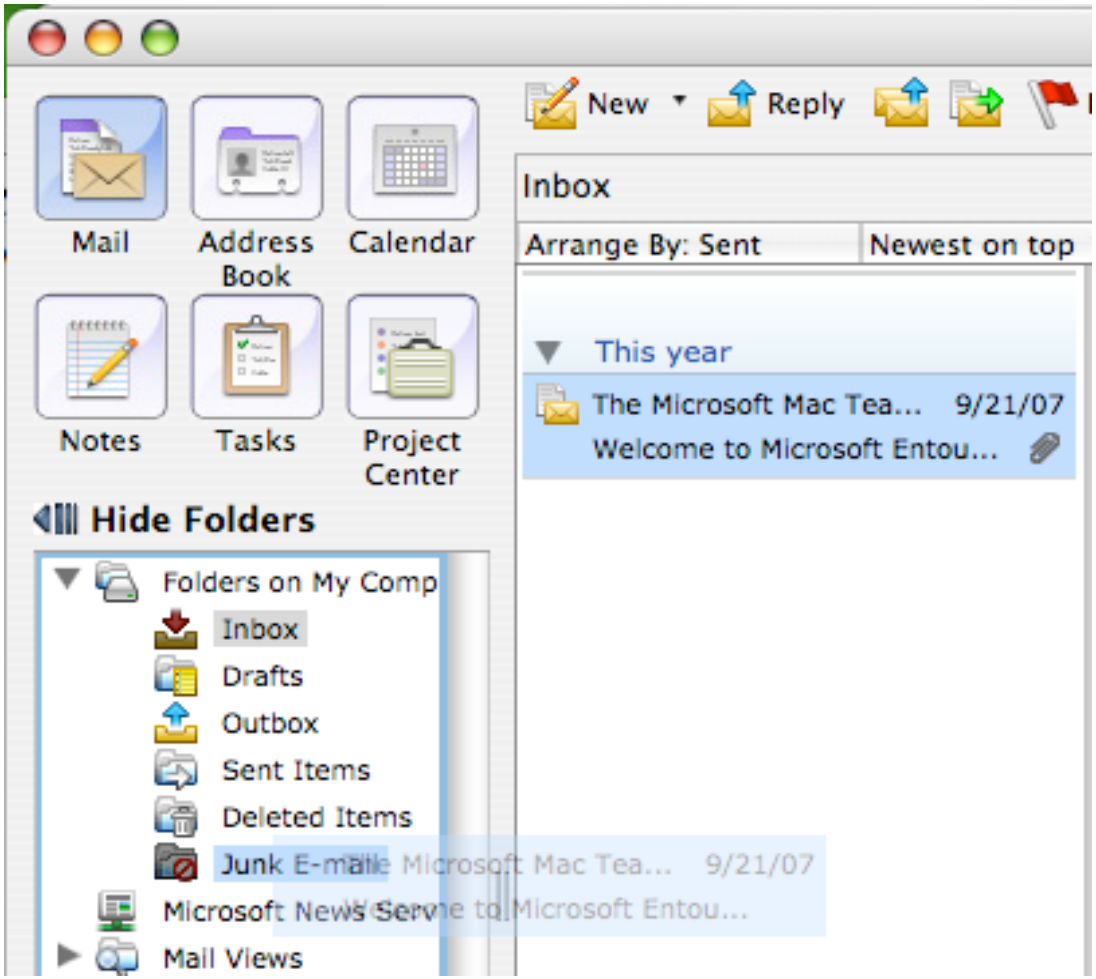
Prevention is preferable.

Your junk mail folder will automatically recognize this sender and block future emails from them!



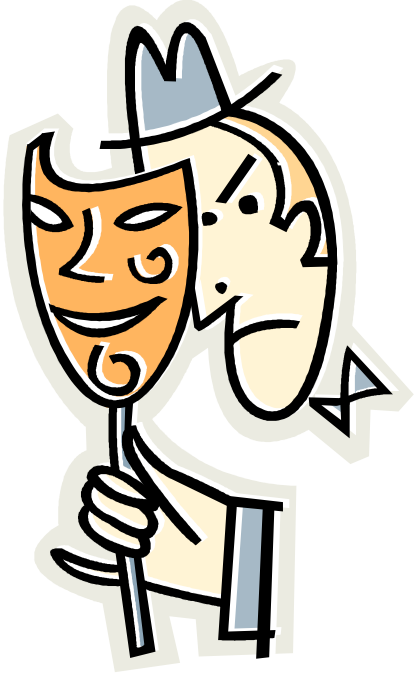
JUNK MAIL

Remember to look inside your junk mail folder periodically to make sure other emails aren't in there by mistake… Drag them out with your mouse.



Another security problem can happen with:

Grades

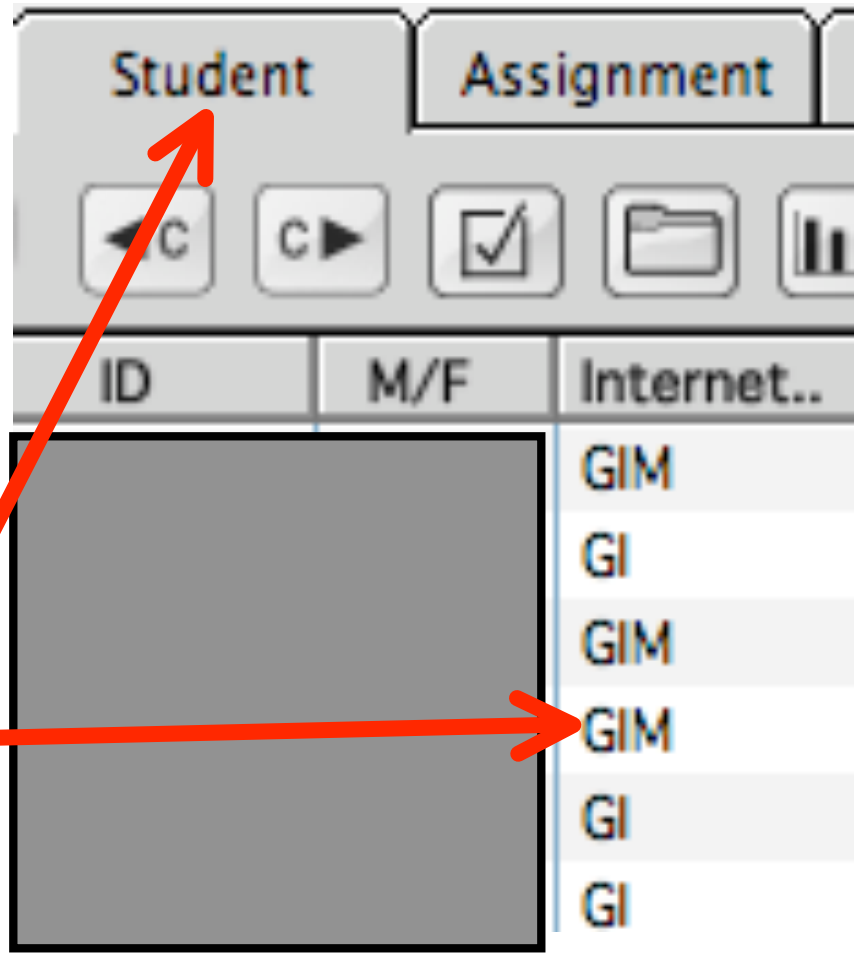


Grades

Do you know when it is **legal** for you to post grades on the internet or send them via email?

Under the Student Menu for EGP:

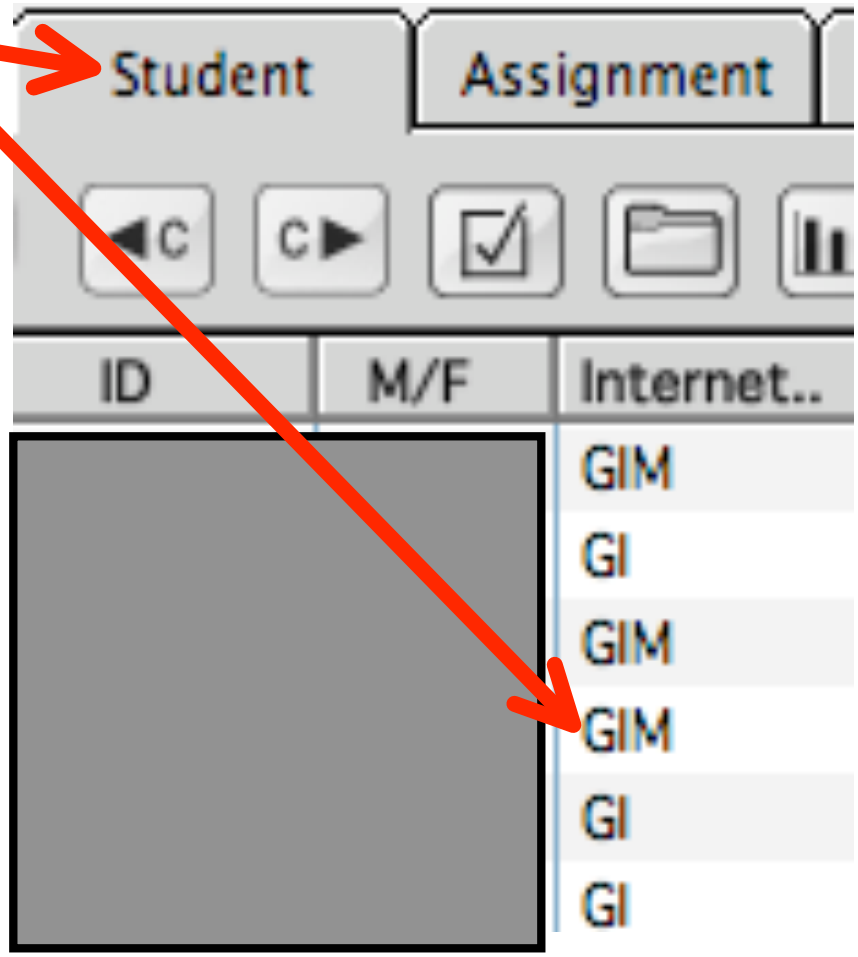
G = grade permission
I = internet permission
M = media permission



Grades

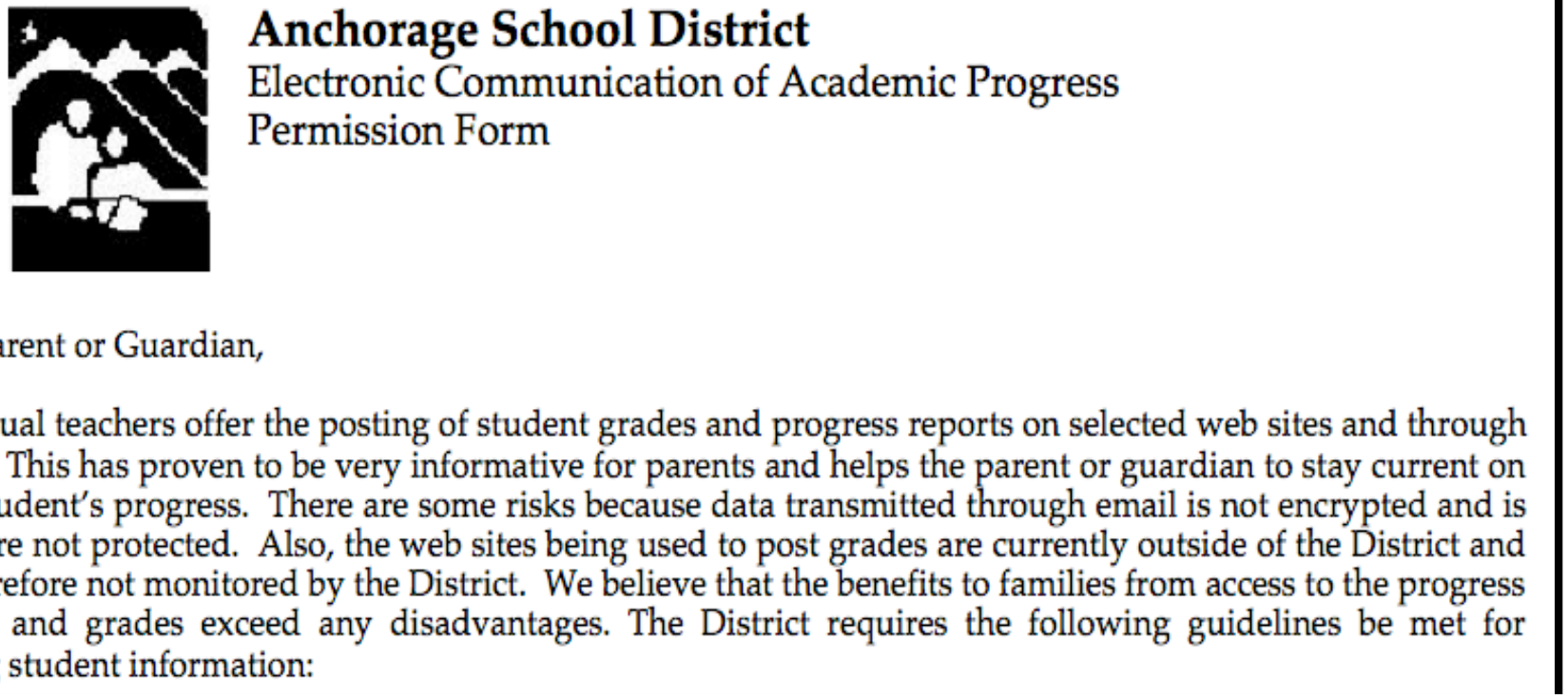
G = grade permission

You are **liable** if you email grades or give a password to students who do not have a **G** here.



Grades

You can send home a permission slip for parents to sign, so you CAN email grades or give a password for online grades.



Anchorage School District
Electronic Communication of Academic Progress
Permission Form

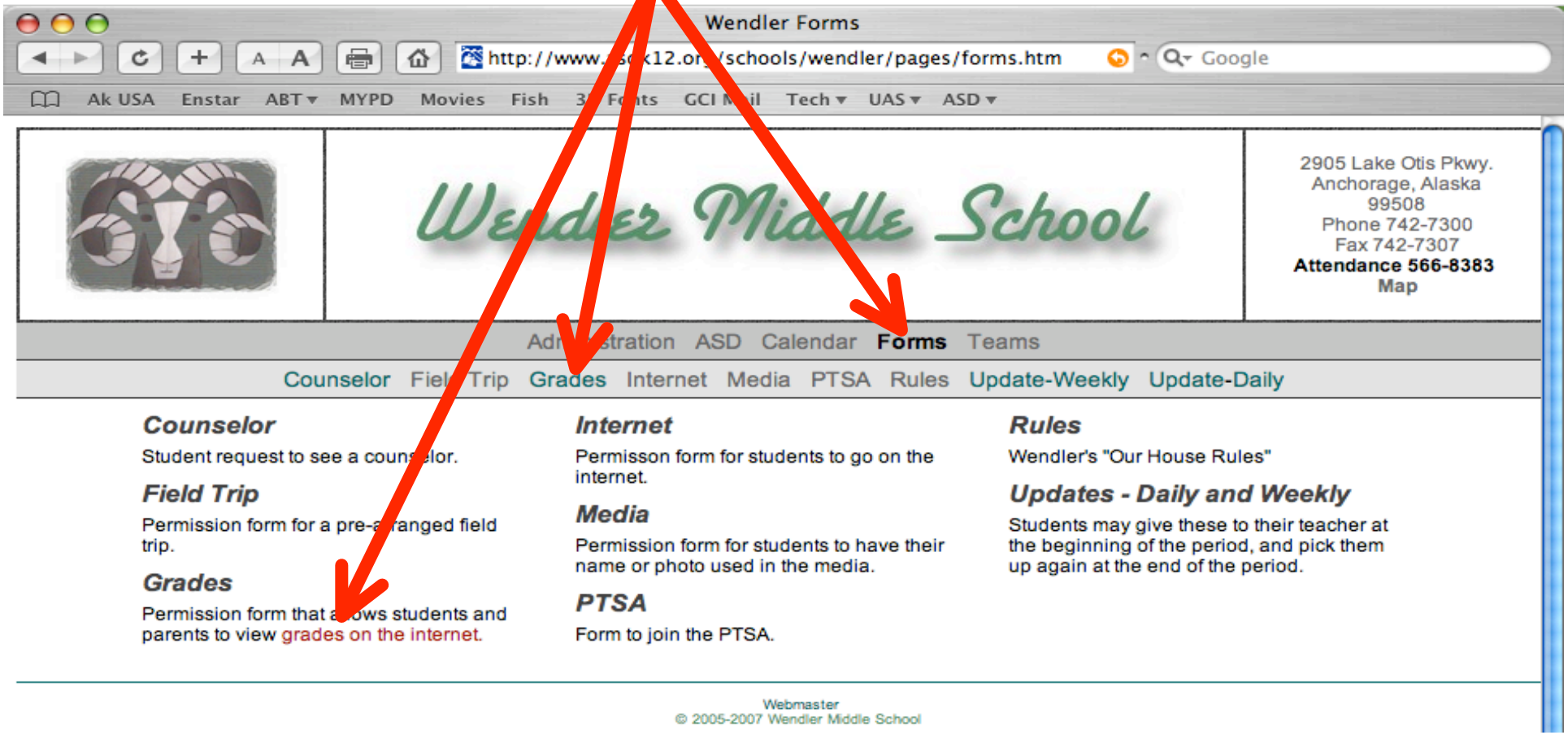
Dear Parent or Guardian,

Individual teachers offer the posting of student grades and progress reports on selected web sites and through email. This has proven to be very informative for parents and helps the parent or guardian to stay current on your student's progress. There are some risks because data transmitted through email is not encrypted and is therefore not protected. Also, the web sites being used to post grades are currently outside of the District and are therefore not monitored by the District. We believe that the benefits to families from access to the progress reports and grades exceed any disadvantages. The District requires the following guidelines be met for posting student information:

Grades

Permission Slip:

http://www.asdk12.org/schools/wendler/pages/forms.htm



Grades

One parent did not want her child's name on the internet for any reason… The EGP user manual (help menu, page 104) says that you can filter out students for uploading to the internet just by deleting their password:

Using Website Reports

Easy Grade Pro's Website Reports are for individual teachers and for schools that want a free and secure way to post student reports for viewing on the internet. Easy Grade Pro creates the reports and the security pages. The reports can then be transferred to your school's web server or to web space provided by an ISP using ftp or some other means.

To gain access to a report, the viewer must enter the student's name and password. Security comes through the use of encrypted student report names and Javascript built into web browsers. For best security, we recommend that reports are not viewed using computers shared by others in a public environment because the browser history stored by web browsers may allow access to reports previously viewed. This risk can be substantially reduced if the browser history is turned off.

To set up Website Reports with password security:

1 Choose Student from the Chart menu and enter passwords in the Password column. Not only are passwords used to gain access to reports on the internet, they are used as filters when creating reports: students without passwords are skipped. Passwords may consist of letters and numbers and must be between six and twenty-four characters in length. They are not case sensitive.

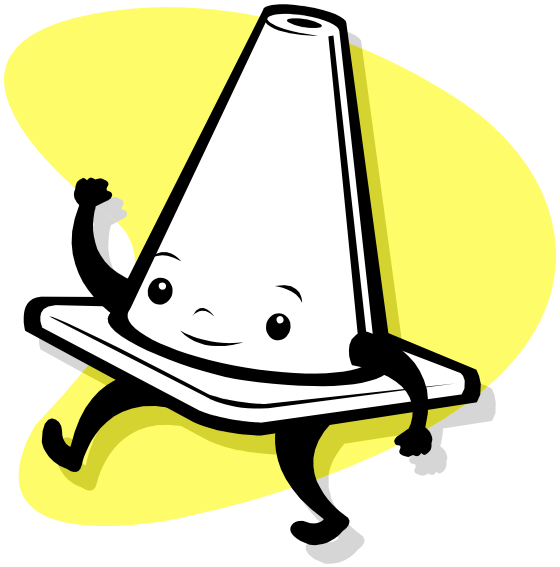
Remember…

Even Apple says, "no computer connected to the Internet will ever be 100% immune from attack…"

http://www.apple.com/getamac/viruses.html

But…

Like driving a car, use some caution and you can protect yourself and your computer.



Resources

ASD Cyber Security
Power Point Presentation:
http://www.asdk12.org/MiddleLink/Internet/CyberSecurity/required.asp

Adapted and Revised for:
Wendler Middle School Staff

Revisions:
Carol Eiben

Editors:
Lisa Sinnot
Patrick Moore